U.S. Department of Justice

Office of the Inspector General

Top Management and Performance Challenges Facing the Department of Justice–2020

October 16, 2020

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 2020 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 nine challenges that we believe represent the most pressing concerns for the Department:

- Strengthening Public Confidence in Law Enforcement and Protecting Civil Liberties
- Use of Sensitive Investigative Authorities by Department Law Enforcement
- The Department's Contingency Planning and Response to a Global Pandemic
- Maintaining a Safe, Secure, and Humane Prison System
- Safeguarding National Security and Countering Domestic and International Terrorism
- Protecting the Nation and Department against Cyber-Related Threats and Emerging Technologies
- The Opioid Crisis, Violent Crime, and the Need for Strong Law Enforcement Coordination
- Ensuring Financial Accountability of Department Contracts and Grants
- Strategic Planning: The Department's Challenges to Achieve Performance-Based Management and to Enhance Human Capital

We believe that strengthening public confidence in law enforcement, protecting civil liberties, and ensuring the proper use of sensitive investigative authorities are urgent challenges that will continue to garner significant attention, and which require appropriate and swift action from the Department. These are not new challenges, and recent events make the Department's attention to them all the more critical. One substantial new challenge facing the Department this year is the need to effectively plan for and respond to the global pandemic

to ensure not only the safety of the public and Department employees, but also that of incarcerated persons.

In addition, enhancing national security remains a key challenge for the Department, particularly given the rising danger of homegrown violent extremism and domestic terrorism. Further, cyber-related intrusions threaten the federal government, the American economy, U.S. public discourse, and American elections. The opioid crisis and violent crime continue to remain challenges for the Department and will require better coordination among all levels of law enforcement to combat them effectively.

The report also highlights the importance of leveraging diversity and inclusion to develop a highly-skilled workforce and thereby ensure employees of all backgrounds are valued and treated fairly.

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.

Strengthening Public Confidence in Law Enforcement and Protecting Civil Liberties

One of the most pressing challenges facing the Department of Justice (DOJ or the Department), in the wake of nationwide protests following the deaths of George Floyd, Breonna Taylor, and Ahmaud Arbery, among other incidents, is how it can most effectively work to strengthen public confidence in law enforcement and protect individuals' civil liberties. This is not a new challenge for the Department. The OIG's 2015 Top Management and Performance Challenges (TMPC) report identified building trust and improving police-community relations as among the most pressing challenges for the Department after police killings of unarmed African Americans in Ferguson, Missouri, and Baltimore, Maryland.

Community trust and cooperation are essential to effective policing. In its dual roles as policy leader and law enforcer, the Department has numerous tools at its disposal to safeguard individual rights and promote constitutional policing practices at the state and local levels. As the nation's leading law enforcement agency, the Department must also ensure that its own law enforcement components, while fulfilling their critical law enforcement missions, adhere to constitutional and statutory constraints designed to protect individuals' civil rights, civil liberties, and privacy.

The Department's efficacy as guardian of the rule of law depends on public confidence that justice is being administered fairly and impartially. Accountability and transparency are critical to building public trust and legitimacy. Robust independent oversight and whistleblower protections can play vital roles in maintaining public confidence in the integrity of the Department and its law enforcement components.

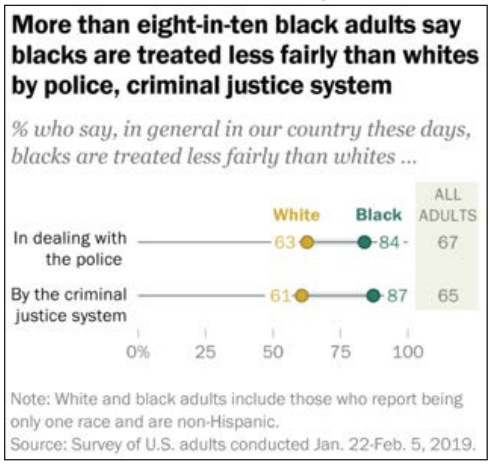
The Department Plays a Critical Role in Ensuring Public Confidence in Law Enforcement

Recent tragic confrontations between police and private citizens—and resulting protests and civil unrest—have brought to the fore a public concern that Black people receive disparate treatment at the hands of law enforcement. A 2019 Pew Research Center survey found that "majorities of both black and white Americans say blacks are treated less fairly than whites in dealing with police and by the criminal justice system as a whole" and that "black adults are about five times as likely as whites to say they've been unfairly stopped by police because of their race or ethnicity."

The Attorney General has heard concerns that "African Americans often feel 'treated as suspects first and citizens second'" and remarked, "I think these concerns are legitimate." In addressing the tension between enforcing the law and upholding the civil rights of all citizens, the Attorney General stated: "While the vast majority of police officers do their job bravely and righteously, it is undeniable that many African Americans lack confidence in the American criminal justice system. That must change. Our constitution mandates equal protection of the laws, and nothing less is acceptable. As the nation's leading federal law-enforcement agency, the Department of Justice will do its part."

Since the OIG published its 2015 TMPC report, Attorneys General have expressed the need to build and maintain community trust in law enforcement. In light of recent events, the need for action to effect actual change is even more urgent. In response to the OIG's 2015 report, the Department identified numerous tools it was using to help build public trust in law enforcement. Those included grant programs to foster partnerships between communities and state and local law enforcement agencies; efforts to improve the collection and analysis of data regarding policing issues such as use of force, traffic stops, and officer-involved shootings; and pattern-or-practice investigations of police departments to root out systemic misconduct and achieve sustainable reform. However, the Department has not fully effectuated the tools it identified in 2015 to address these issues and, in some cases, has cut back on their use. We believe that among the most significant challenges facing the Department is responding to the potential erosion of confidence in law enforcement, as evidenced by the Pew study, as well as embracing its leadership role and using all available tools to address these issues to the fullest extent practicable.

Public Perception of Fairness in the Criminal Justice System



Source: "10 Things We Know About Race and Policing in the U.S." Pew Research Center, Washington, D.C. (June 3, 2020)

Although the Department has no direct authority over law enforcement agencies other than its own, as both a law enforcer and policy leader, the Department has numerous mechanisms to help protect individuals' civil liberties and strengthen public confidence in law enforcement at all levels. Among them are the Presidential Commission on Law Enforcement and the Administration of Justice, criminal and civil enforcement targeting civil rights violations by police, leading by example through the DOJ law enforcement components, and grants and technical assistance to promote cultures of integrity and build public trust in policing.

Presidential Commission on Law Enforcement and the Administration of Justice. In January 2020, the Department established the Presidential Commission on Law Enforcement and the Administration of Justice (the Commission). While the Commission's report has not been released as of this writing, the Commission has held panels on community engagement, trust and respect for law enforcement, and policing culture. At a June 24 hearing on the use of force and culture change, the panelists acknowledged that, "while no single police incident represents an entire department, nothing undermines years of work developing community trust as quickly as incidents where police use unnecessary or excessive force."

While the Commission has the potential to influence the national conversation, its efficacy will ultimately turn on whether the public views its recommendations as legitimate. In an amicus curiae brief filed in June, some current and former prosecutors and law enforcement officials alleged that the Commission lacks transparency and representation from key stakeholders, such as civil rights groups and police reform advocates. Some of the Commission's working group members have raised similar concerns and, in September, one prosecutor resigned from his working group after the prosecutor said the Commission failed to address the problems he and another member had identified. Additionally, on October 1, a federal judge ruled the Commission in violation of the federal law governing advisory commissions, finding, among other things, that its membership is not "fairly balanced" in the viewpoints represented. The judge ordered the Commission to halt all work and not to release its report

until it comes into compliance with the law. Such criticisms and findings, if left unaddressed, may undermine public confidence in the Commission's work. The challenge to the Department will come in its presentation of and response to the Commission's final report.

Criminal and Civil Enforcement Targeting Civil Rights Violations by Police. The Department's Civil Rights Division (CRT) has authority under 18 U.S.C. § 242 to prosecute individual law enforcement officers for willful civil rights violations. CRT also has authority, under 34 U.S.C. § 12601 (formerly 42 U.S.C. § 14141), to investigate police departments for patterns or practices of unconstitutional policing and to bring civil enforcement actions or seek other forms of relief where such pattern or practice is found. In June 2020, CRT took a positive step forward by launching a "Civil Rights Reporting Portal," which makes it easier for the public to report civil rights violations, including misconduct by law enforcement officers. Given recent events, however, there have been bipartisan calls for the Department to maximize use of its pattern-or-practice authority to establish accountability and public trust in law enforcement. The Department faces challenges in balancing its stated policy favoring local control and local accountability over nonfederal law enforcement agencies with the need to assure the public that the Department is using its available authorities to vindicate and prevent civil rights violations in policing at the state and local levels.

Leading by Example Through the Department's Law Enforcement Components. The Department's law enforcement components provide crucial assistance to state and local law enforcement agencies responding to civil unrest. The Department must ensure, however, that in doing so its law enforcement components respect the civil rights and civil liberties of peaceful protesters exercising their right to free expression. The Department's Annual Performance Plan for Fiscal Year 2021 identified defending the First Amendment right to free speech as one of the Department's top strategic objectives.

The federal government's response to recent protest activity in Washington, D.C., and Portland, Oregon, generated civil rights lawsuits against the DOJ and other federal agencies. In response to requests from Congress and the public, the OIG has initiated a review into the Department's actions in Washington and Portland and is also investigating use-of-force allegations involving DOJ law enforcement personnel in Portland. The review will include "examining the training and instruction that was provided to the DOJ law enforcement personnel; compliance with applicable identification requirements, rules of engagement, and legal authorities; and adherence to DOJ policies regarding the use of less-lethal munitions, chemical agents, and other uses of force." Separately, the Department of Homeland Security (DHS) OIG has announced the initiation of an investigation regarding DHS law enforcement activity in Portland, and the Department of the Interior (DOI) OIG has announced that it is investigating DOI law enforcement activity in Washington, D.C. The OIG is coordinating with the DHS and DOI OIGs in the respective investigations in Portland and Washington, D.C.

The Department must also work to ensure that, in exercising its law enforcement authorities, its components adhere to policies designed to protect individuals' privacy. A recent OIG review and follow-on audit work found serious deficiencies in a number of the Federal Bureau of Investigation's (FBI) applications for warrants under the Foreign Intelligence Surveillance Act (FISA). Such deficiencies can damage the public's confidence in the FBI and the Department as a whole. The Use of Sensitive Investigative Authorities section of this report discusses FISA and the OIG's findings in more detail.

Office of Community Oriented Policing Services. The Office of Community Oriented Policing Services (COPS) provides another avenue for strengthening public confidence in law enforcement. The COPS Office offers a number of resources to help police departments build community trust and has, in the past, sponsored competitive grant programs aimed at enhancing cultures of integrity in policing. Since 2011, the COPS Office has provided training and technical assistance to state and local law enforcement agencies through the Collaborative Reform Initiative Technical Assistance Center (CRI-TAC) program, which was created to help law enforcement agencies address issues that impact public trust, such as use of force, racial profiling, and other areas of concern. In 2017, however, the Department revised CRI-TAC's role to focus on public safety and combatting violent crime. Because building trust and mutual respect between police and communities is critical to public safety, efforts to reduce violent crime should go hand in hand with programs to strengthen public confidence in law enforcement.

Improving Transparency and Accountability in Law Enforcement

Body-worn Cameras and Law Enforcement Identification. Body-worn cameras (BWC) are one tool available to law enforcement to improve transparency and accountability and, thereby, build the trust of the communities they serve. According to OJP, since 2015, the Department's Bureau of Justice Assistance has provided more than $113 million to state, local, and tribal agencies through its Body-Worn Camera Policy and Implementation Program, with over $20 million provided in fiscal year (FY) 2019 alone. As a policy leader, the Department can set an example for BWC use by establishing effective policies and practices for its own law enforcement components. In October 2019, the Department announced a pilot program that will allow federally deputized task force officers to use BWCs while conducting arrests or executing search warrants. The OIG is currently auditing the Department's policy and practices on BWC use among its law enforcement components and federally deputized task force participants.

Recent events have also centered public attention on the issue of law enforcement identification. In June 2020, reports emerged that some federal law enforcement officers deployed to assist at protests in Washington, D.C., did not wear badges or other identifying information and, in some instances, allegedly refused to identify themselves when asked. Such reports have raised concerns about individuals' ability to hold unidentified law enforcement officers accountable for potential civil rights violations. Congress is considering bills that would require federal law enforcement officers to display identifying information and to identify themselves before using force. The Department must assure the public that its law enforcement components can be held accountable for actions they take while seeking to enforce the law.

Statutorily Independent Oversight of Department Lawyers. Another means of strengthening confidence in law enforcement is ensuring vigorous independent oversight of all stages of the Department's enforcement efforts. To that end, Congress is currently considering a bipartisan bill that would expand the OIG's jurisdiction over certain attorney misconduct matters that are at present exclusively within the jurisdiction of the Department's Office of Professional Responsibility, "a DOJ component that lacks the same statutory independence and protections the OIG is provided." Whether or not that bill becomes law, it is imperative that the Department welcome and encourage independent oversight as a means to foster accountability and public trust.

Robust Whistleblower Protections. Relatedly, the Department must work to ensure that whistleblowers feel free to come forward with allegations of wrongdoing without fear of retaliation or reprisal. As the Council of the Inspectors General on Integrity and Efficiency stated last year, "Because the effectiveness of our oversight work depends on the willingness of government employees, contractors, and grantees to come forward to us with their concerns about waste, fraud, abuse, and misconduct within government, those individuals must be protected from reprisal."

The Department continues to face challenges in ensuring that its employees, contractors, and grantees respect the role and rights of whistleblowers. Within the past year, the OIG has found three instances in which a government or contractor employee suffered reprisal for making protected disclosures or reporting alleged ethics violations. In addition, the OIG has recently issued recommendations to the Federal Bureau of Prisons (BOP) and the U.S. Marshals Service (USMS) to ensure that their respective contractors are aware of and are abiding by whistleblower protection laws. Several recent OIG audits have also uncovered whistleblower-related noncompliance in contracts awarded by DOJ components, including the Drug Enforcement Administration (DEA), the BOP, the Environment and Natural Resources Division, the USMS, and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). As the DOJ Inspector General recently testified before the House Oversight Committee, "Whistleblowers perform an essential public service in ensuring accountability in government, and it is therefore critically important that protections from retaliation be meaningful and robust."

Use of Sensitive Investigative Authorities by Department Law Enforcement

The Department's law enforcement components are tasked with complex investigations, some of which have implications for national security, or involve transnational or domestic criminal enterprises. As an aid in conducting such critical investigations, components have been granted authority to use a variety of sensitive investigative techniques, including electronic surveillance, confidential sources, undercover activities, and activities that may otherwise be illegal. While using these tactics may be an effective means to disrupt national security threats or the activities of criminals, they present substantial risks to the Department. The risks arise from reliance on the invasiveness of the techniques affecting individuals' privacy, persons with mixed motives and a history of involvement with questionable associates, activities that could endanger civilian lives, and the authorized furthering of criminal activity. Department management's challenge is to ensure appropriate controls are in place to mitigate these risks and increase the likelihood that use of sensitive investigative techniques is productive in advancing the most serious national security and criminal investigations.

The Department's Strategic Management and Oversight of Confidential Sources

Law enforcement components utilize Confidential Sources (CS) in criminal and national security investigations to identify investigative targets or infiltrate organizations representing a threat to the safety and security of our communities. However, the use of CSs is inherently risky. In FYs 2016 through 2020, the OIG reviewed the protocols for the use of CSs by the three largest Department law enforcement components, the FBI, ATF, and the DEA. Each of these audits identified significant deficiencies in internal controls, and questionable strategic uses of CSs. Common deficiencies included a lack of oversight in the CS validation process, inability to track CS payments, and inadequate management of CS activity. To mitigate such risks, the OIG recommended the Department components that were reviewed develop and implement appropriate CS monitoring, which the Department, DEA, and ATF have since resolved and closed. The OIG remains concerned about this sensitive investigative technique and the similarity of the findings present throughout these law enforcement components.

The most recent of these reviews, was the OIG's Audit of FBI's Management of its Confidential Human Source Validation Processes, issued in November 2019. During this review, the OIG found that the validation unit did not document instances that could result in the reporting of derogatory information about CSs. We also found that the FBI lacked an automated process to analyze its CS coverage to address intelligence gaps, as similarly reported in a 2016 audit of the DEA's CS program. The Department's ability to deploy appropriate resources, such as CSs, to investigations is critical to the success of operations. In addition, during the OIG's Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation (Crossfire Hurricane), issued in December 2019, we found serious lapses in the FBI's handling of one CS. In view of the high-profile nature of that particular investigation, one would expect rigorous adherence to policy and guidelines. We found that was not the case. The OIG expressed concern regarding the lack of plan in place to address the possible collection of politically sensitive information by CSs and the lack of FBI policy requiring Department consultation prior to tasking CSs with consensually monitoring conversations

with members of a presidential campaign. The Department components' efforts to close the OIG's recommendations in this area will assist it in mitigating the risks associated with the use of this valuable but perilous investigative authority. In response to the OIG's reports and recommendations, the FBI has nearly completed implementing a series of CS policy revisions designed to address the issues we identified.

In addition to operational risks facing the Department, the OIG continues to identify issues related to internal controls over CSs. Similar to our findings from previous DEA and ATF audits, in the November 2019 FBI audit we found that the FBI failed to follow established policies regarding communication practices with CSs and lacked required Department oversight at meetings. Additionally, we noted the Attorney General Guidelines governing CSs may not adequately reflect current operational risks. The OIG recommended that the FBI design, implement, and adhere to procedures for its long-term CSs that comply with the AG Guidelines, or coordinate with the Department to seek revisions to the AG Guidelines, as necessary. The FBI has met with the Department regularly on this issue and is actively engaged in collaboration with the Department to finalize changes to the AG Guidelines.

Not only were issues present within law enforcement components' long-term CSs, the OIG has also identified issues with the Department's use of immigration sponsorship to support criminal investigations and prosecutions, often facilitated through CS programs. In a June 2019 report, we found that the Department was not adequately monitoring DOJ-sponsored foreign nationals and we identified 62 sponsored foreign nationals who had absconded from DOJ control. As of September 2020, some Department components had not closed the recommendations to improve policies and processes to better track foreign national sponsorship information.

Because the OIG has audited DOJ component's CS programs and continued to find strategic and administrative issues, the Department should continue to assess the risk of using CSs and enhance oversight procedures over these programs. The OIG will continue to conduct oversight work in this area to provide assistance to the Department's efforts to effectively manage the associated risks.

Oversight of the Use of the Foreign Intelligence Surveillance Act

The Department's authority under the Foreign Intelligence Surveillance Act (FISA) to conduct electronic surveillance and physical searches is a powerful investigative tool that also raises civil liberties concerns. FISA orders can be used to surveil U.S. persons, and proceedings before the Foreign Intelligence Surveillance Court (FISC) inherently exclude the party surveilled. In light of this process, the Department and FBI have established procedures and safeguards, including the requirements in FBI policy that every FISA application contain a "full and accurate" presentation of the facts and that all factual statements in FISA applications are "scrupulously accurate."

The OIG's recent work has raised serious concerns about the accuracy of the Department's submissions to the FISC and the FBI's compliance with its FISA policies and procedures. In the OIG's Review of Crossfire Hurricane, the OIG found that the FBI and Department failed to meet their basic obligation of accuracy. In four applications targeting Carter Page, a former Trump campaign advisor, the OIG found at least 17 significant inaccuracies and omissions in the applications' statements of facts supporting probable cause. As a result, relevant information was not shared with Department decision makers and the FISC, and the applications made it

appear that the evidence supporting probable cause was stronger than was actually the case. Due to the many basic and fundamental errors that were made by separate teams on highly sensitive FISA applications (which FBI officials expected would be subjected to close scrutiny), the OIG concluded the investigation raised significant questions regarding the FBI chain of command's management and supervision of the FISA process.

Following this review, the OIG initiated an audit to examine the FBI's compliance with its internal procedures, known as the Woods Procedures, to ensure accuracy of FISA applications. The OIG's audit focused on FISA applications targeting U.S. persons. In March 2020, the OIG issued a Management Advisory Memorandum (MAM) to the FBI in which we reported that of 29 FISA applications judgmentally sampled by the OIG, 4 applications were missing Woods files and the remaining 25 contained apparent errors or inadequately supported facts. The MAM also reported that the FBI had previously identified similar deficiencies in support for FISA applications, but that these accuracy reviews had not been used strategically to help assess the FBI's compliance with its Woods Procedures. The OIG's Woods Procedures audit is continuing. We anticipate making further recommendations to the FBI to strengthen its controls over this important and highly sensitive authority.

In light of the OIG's work, the FISC has issued several orders stating that the FBI had failed to meet its duty of candor and requiring the government to inform the FISC what it is doing to ensure that FISA applications are accurate. On August 31, 2020, in part as a result of the OIG's work, the Attorney General issued two memoranda that authorized the establishment of an FBI Office of Internal Auditing (OIA), ordered the development of compliance and oversight mechanisms and other internal controls, and created additional protocols designed to ensure the accuracy and completeness of FISA applications. As noted in the Attorney General memorandum establishing the OIA, the Inspector General agreed to assess the FBI's compliance with the memorandum within 18 months after the establishment of the OIA, to conduct a subsequent assessment within 5 years after the initial assessment, and to review the FBI Office of General Counsel's role in overseeing compliance with applicable laws, policies, and procedures relating to the FBI's national security activities. The OIG's work in this area can substantially assist the Department and FBI in addressing concerns raised by the FISC, Congress, and the American public about the use of FISA surveillance authority, particularly against U.S. persons.

"FISA is an indispensable tool that the FBI uses to protect our country from national security threats, and Americans can rest assured that the FBI remains dedicated to continuously strengthening our FISA compliance efforts and ensuring that our FISA authorities are exercised in a responsible manner."

–FBI Director Christopher Wray

The Department's Risk Assessment Practices Within Component Undercover Operations

Law enforcement components within the Department organize and implement undercover operations to infiltrate criminal enterprises. These operations often allow undercover agents or CSs to perform activities that would otherwise, without proper approval, be considered illegal. Because these activities may involve the very crimes that these components are investigating, the Department must ensure each component operates with a strong internal control framework. Based on findings from the OIG's 2012 review of the Department of Justice's and ATF's Implementation of Recommendations Contained in the OIG's Report on

Operations Fast and Furious and Wide Receiver and subsequent 2016 follow up, Department executives created protocols for assessing risk during investigations such as initiating and overseeing Sensitive Investigative Activities, using CSs, authorizing Otherwise Illegal Activities by Undercover Agents or Informants, and a series of controls for income-generating operations.

> **"Given the risks and sensitivities associated with AGEOs and the frequency with which they are used, we believe that it is essential for the Department to have an appropriately rigorous body of policy to help ensure that the risks are mitigated consistently and adequately by all DOJ law enforcement components."**
>
> **-OIG Audit of the DEA's Income-Generating, Undercover Operations**

Despite this guidance, the OIG's June 2020 Audit of the DEA's Income-Generating, Undercover Operations, known as Attorney General Exempt Operations (AGEO), found that these undercover operations exhibited issues reflecting continued ineffective oversight and management. The OIG highlighted that, "while the ultimate goals of AGEOs support the DEA's mission, the collateral consequence of assisting the basic operation of drug trafficking and money laundering organizations does not. The DEA and DOJ must improve AGEO guidance, oversight, and management to ensure that the benefits outweigh risks of the DEA engaging in authorized illegal activities." In fact, the DOJ indicted a former DEA special agent and his spouse for their alleged roles in a scheme to divert drug proceeds sourced from undercover money laundering investigations to personal bank accounts, and in September 2020, the former DEA special agent pled guilty to a 7-year scheme diverting $9 million in drug proceeds. These issues parallel oversight and management issues discovered within AGEOs at ATF in 2013, in which we found significant internal control deficiencies leading to investigations lacking specific direction and at risk for misuse of funds. The OIG is currently auditing the FBI's National Security Undercover Operations as part of our efforts to address the risks in this area.

In addition to the aforementioned subjects, the OIG has previously conducted work, highlighted challenges, and is conducting ongoing work related to other sensitive investigative techniques, such as bulk data collection, facial recognition technology, the use of National Security Letters, and the use of foreign law enforcement to aid in operations. As we noted in the FY 2019 TMPC, 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 found that the DEA proceeded without sufficient legal analysis of its subpoena authority and without adequate procedural safeguards. As of March 31, 2020, the 16 review recommendations were on hold and or pending with the OIG. The Department's responses to OIG reviews have improved its oversight of its use of sensitive authorities. In addition, corrective action taken by the FBI as a result of the OIG's reports regarding the FBI's use of National Security Letters and USA PATRIOT Act section 215 authorities has substantially enhanced oversight of the use of these investigative tools and reduced the risk of their misuse.

Overall, while the Department and components have indicated that sensitive investigative authorities are successful tools to combat threats, the use of these techniques must be tempered by sufficient controls. As reflected in the recommendations we have made in our numerous reviews of the use of sensitive investigative authorities, the OIG considers the strategic management, risk mitigation, and internal controls over the existing activities and operations noted above to be of paramount importance to the Department as it seeks to disrupt national security and criminal threats.

The Department's Contingency Planning and Response to a Global Pandemic

Responding to the rapidly evolving coronavirus disease 2019 (COVID-19) pandemic presents immediate and significant challenges for the Department, most notably in its responsibility to keep its employees, contractors, visitors, and workspaces as safe as possible. In addition to protecting its own workforce while also performing its enforcement and national security responsibilities, the Department faces growing pandemic-related challenges that include: preventing the spread of the virus among the roughly 155,000 federal inmates and 61,000 detainees in BOP and USMS custody, respectively; ensuring robust oversight of $850 million in Coronavirus Aid, Relief, and Economic Security Act (CARES Act) grant funding being disbursed by the Department to fund state, local, and tribal efforts to prevent, prepare for, and respond to COVID-19; combatting COVID-19-related fraud, scams, and violations of federal antitrust and other laws; and operating the nation's immigration courts in a manner that minimizes risk to participants while preserving individual rights. As the global pandemic continues to evolve, so, too, must the Department's response.

> **"Our country now faces a challenge the likes of which none of us have ever experienced. The coronavirus has upended every American's daily life. It threatens the health of every man, woman, and child. It has disrupted business, our basic social interactions, and how government goes about doing the work of the people."**
>
> **Deputy Attorney General Jeffrey A. Rosen, April 29, 2020**

Department Workforce Challenges

The Department employs over 115,000 personnel worldwide executing the federal government's law enforcement and national security efforts. A principal challenge for the Department is ensuring that these mission critical functions continue to operate effectively during the global pandemic while protecting the health and safety of its employees. This may be particularly challenging given the nature of the Department's investigative and classified work. The Department's core investigative operations have continued throughout the pandemic, with critical employees continuing to report to their workplace. Department employees conducting investigative work face higher risks of exposure to COVID-19, not only from reporting to the workplace but also because they must continue to interact with witnesses and subjects and make arrests. To gain a better understanding of the impact of COVID-19 on the Department's investigative operations, the OIG is currently conducting a survey of ATF, the DEA, the FBI, U.S. Attorneys' Offices, and the USMS.

Many Department employees have worked remotely throughout the pandemic and will likely continue to do so for months to come. Internal and external technological challenges, including information technology (IT) connectivity, have impacted the productivity of these employees. As mass telework continues, components are overcoming some of these challenges. However, the Department's pandemic response has highlighted how some of DOJ's IT services are fragmented or need modernization to perform optimally. In addition,

the lack of mobile classified computing capabilities has hampered the Department's national security work and has necessitated that employees return to the workplace to perform classified work. Further, senior Department leadership communications have been hampered due to the lack of a Department-wide command and control system, and several DOJ components remain unable to fully leverage common virtual collaboration tools Department-wide. The combination of these IT gaps highlights the need for the Department to focus on its enterprise IT capabilities, which will improve the day-to-day mission capabilities of the Department and better position it to perform during a crisis.

As these employees begin returning to the workplace, the Department will face challenges that include accommodating social distancing practices, managing the presence of visitors (including witnesses and inmates) in the workplace, establishing contact tracing protocols in the event of an employee or visitor infection, and instituting enhanced cleaning requirements. In June 2020, the Department issued best practices to prepare for the phased return to DOJ workplaces, which included guidance on face coverings, social distancing, and temperature screening. As the pandemic continues, the Department may continue to face challenges as its employees manage issues such as childcare and high-risk individuals in their households.

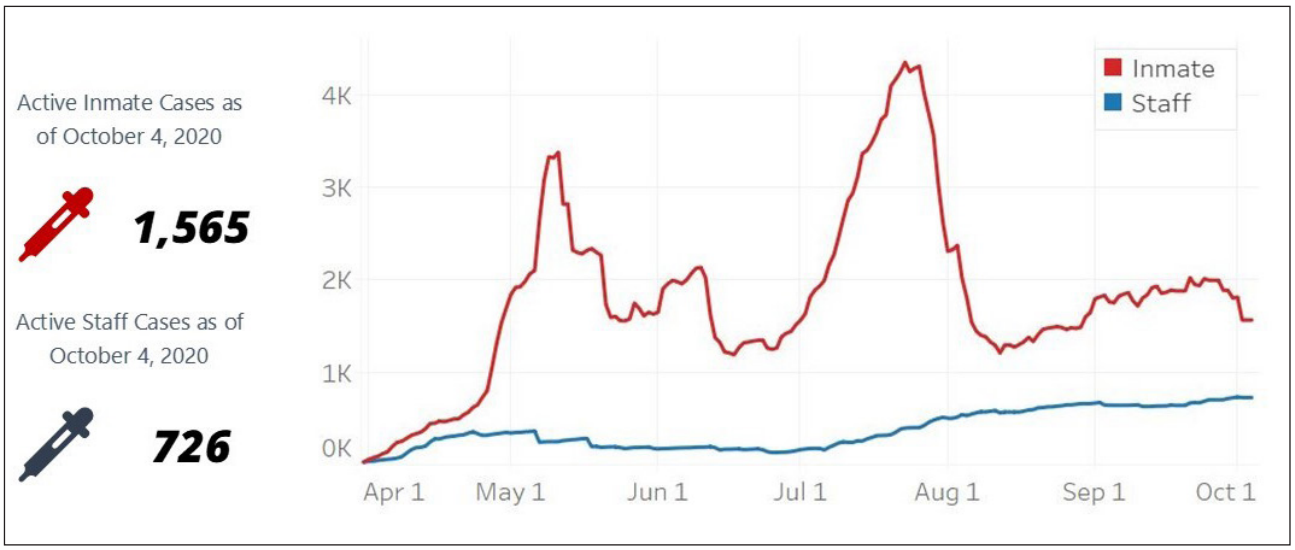
Protecting the Health and Safety of BOP and USMS Staff, Inmates, and Detainees While Maintaining Operations

In April 2020, the OIG determined that one of the most significant challenges the Department faces is protecting the safety and welfare of BOP inmates, staff, and the communities in which they serve. As of October 2020, the Department housed roughly 155,000 federal inmates and employed approximately 37,000 staff and contract employees in federal prisons, contract prisons, and residential reentry centers.

In April 2020, the OIG initiated a series of 16 remote inspections of facilities housing BOP inmates to both assess their compliance with available guidance and best practices for managing COVID-19 and assist the BOP in mitigating the health risks arising from the pandemic. On July 23, the OIG issued its first two remote inspection reports, concerning the Federal Correctional Complex (FCC) Lompoc in Santa Barbara, California, and FCC Tucson in Pima County, Arizona. Those reports presented very different situations at those two facilities, in terms of both numbers of staff and inmates infected with COVID-19 and how the respective institutions prepared for and managed COVID-19 outbreaks.

As of October 2020, approximately 18 percent of BOP inmates were housed in contract prisons and residential reentry centers—correctional environments not directly controlled by the Department. This can present additional challenges. For example, in its August 2020 remote inspections of three BOP contract prisons, the OIG found that contract prisons received most BOP guidance documents between 1 and 5 days after comparable guidance was issued to BOP-managed institutions, but some delays were more significant. The OIG will release the remaining 11 remote inspection reports in the near future and also plans to prepare a capstone report providing BOP-wide conclusions and recommendations resulting from its inspections. In addition, as shown below, the OIG launched an interactive collection of dashboards providing data relating to COVID-19 within the BOP.

Active BOP COVID-19 Cases Over Time, March 31–October 4, 2020



Source: BOP

Correctional facilities, by their very nature, can make containing a highly contagious virus difficult because they are designed to keep inmates in close or confined quarters. As the BOP continues to modify its operations to control COVID-19 transmission in its facilities, it must ensure that it issues timely guidance to staff at all facilities housing BOP inmates; addresses pre-pandemic health services and correctional staffing shortages to meet inmates' medical and mental health needs; maintains adequate supplies of personal protective equipment (PPE); maintains effective protocols for COVID-19 testing, quarantine, medical isolation, and use of PPE protocols; and continues employing social distancing strategies.

Further compounding these challenges is an aging inmate population that exhibits higher rates of underlying health conditions compared to the general population. On April 3, 2020, the Attorney General, under authority granted him by the CARES Act, directed the BOP to maximize transfers of all appropriate inmates to home confinement, particularly from facilities where COVID-19 materially affected operations. As of October 14, 2020, the BOP reported that it has transferred 7,784 inmates to home confinement. However, during the early stages of the pandemic, we found instances where the BOP was slow to use this authority to mitigate the effects of COVID-19 by reducing the inmate population. The OIG's remote inspection of FCC Lompoc found that its use of home confinement to contain the spread of COVID-19 at the facility was limited: although over 900 Lompoc inmates had contracted COVID-19 as of May 13, 2020, only 8 had been transferred to home confinement under the CARES Act. In light of these findings, the OIG is also currently assessing the Department's and the BOP's use of early release authorities to manage the spread of COVID-19 across its institutions.

In addition to the BOP, as of August 2020 the USMS was overseeing over 61,000 detainees awaiting trial or sentencing decisions, about 70 percent of whom were held in over 850 different state, local, or tribal facilities under the terms of intergovernmental agreements. Of particular concern is the USMS's decentralized system, which creates potential safety issues as detainees are transferred between facilities and to and from federal courthouses and U.S. Attorney's Offices. To assist the USMS in mitigating health risks, the OIG is conducting a review of the USMS's response to the COVID-19 pandemic to assess compliance with available guidance and best practices for preventing, managing, and containing potential COVID-19 outbreaks in its detention settings.

Oversight and Administration of CARES Act Funding

The CARES Act, which was signed into law on March 27, 2020, appropriated $1.007 billion to the Department to respond to the COVID-19 pandemic. Of the $1.007 billion, $850 million (84 percent of the total) was allocated to the Department's Office of Justice Programs (OJP) to award grants to fund eligible states, units of local government, federally-recognized tribes, U.S. territories, and the District of Columbia to prevent, prepare for, and respond to the COVID-19 pandemic. As noted in the OIG's June 2020 Pandemic Response Report, recipients of OJP's Coronavirus Emergency Supplemental Funding (CESF) awards will be operating under unprecedented circumstances, including reductions in administrative staff that may weaken internal control systems. The OIG is currently reviewing OJP's administration of CARES Act funding to assess OJP's efforts to distribute CESF funding in a timely and efficient manner and determine whether CESF awards were made in accordance with applicable laws, regulations, and other guidelines.

In July 2020, the OIG issued an interim report on OJP's administration of CARES Act funding, which found that OJP had distributed CESF awards quickly and in accordance with CARES Act requirements. The OIG did identify two areas of concern specific to the CESF program. First, the OIG found that some local CESF awards had gone to areas with few reported positive COVID-19 test results. Although the report noted that "in and of itself, this is not an indicator that the funding will be used for unallowable purposes," it found that "OJP's CESF monitoring strategy may benefit if oversight protocols consider factors such as recipients who are in areas with few positive COVID-19 test results or deaths." Second, the OIG found that the CESF program is vulnerable to fraud schemes and stated that "OJP should consider providing regular updates of known fraud schemes to its CESF community." According to OJP, it has taken actions to address the concerns identified in the OIG's interim report, including posting information about fraud schemes on its website.

The OIG will continue to issue periodic focused interim reports regarding OJP's administration of CARES Act funding, to both provide transparency to the public and ensure that OJP can review and respond to areas of potential risk in a timely manner.

Combatting COVID-19-Related Fraud, Scams, and Violations of Federal Antitrust Laws Through Effective Enforcement

The CARES Act and other pandemic related funding have resulted in the spending of over $2.6 trillion. As a result, the Department's law enforcement components will face increased demands in identifying and prosecuting opportunists attempting to exploit the COVID-19 pandemic funding through frauds and other scams that harm the public, while continuing to combat its non-COVID related law demands. In March 2020, the Department warned the business community of its intent to hold accountable those who violate antitrust laws in connection with the manufacture, distribution, or sale of public health products such as face masks, respirators, and diagnostics. The Department is coordinating the efforts of its law enforcement components with the Pandemic Response Accountability Committee and Inspectors General communities related to stimulus funds fraud. The Department's Procurement Collusion Strike Force—a partnership with federal, state, and local government agencies the Antitrust Division established in November 2019 to target violations of criminal antitrust laws in the competitive bidding process—has also worked to identify collusion and other COVID-19 related criminal schemes that impact public procurement. Additionally, in March 2020, the Attorney General directed the creation of a COVID-19 Hoarding and Price Gouging Task Force to "aggressively pursue bad actors who amass critical supplies either

far beyond what they could use or for the purpose of profiteering." In September 2020, the Acting Assistant Attorney General for the Criminal Division, in speaking about the Paycheck Protection Program, noted that "any time the federal government makes a large amount of money available to the public on an expedited basis, the opportunities for fraud are clear."

The OIG has identified a variety of pandemic-related criminal schemes, including online scams, fraudulent medical equipment sales, and COVID-19 treatment and cure scams, among others. According to the FBI, as of September 2020, the FBI's Internet Crime Complaint Center had received and reviewed more than 22,000 complaints related to COVID-19 fraud, many of which concerned websites that advertised fake vaccines and cures, operated fraudulent charity drives, or delivered malware. In August 2020, the Department announced that it had obtained a temporary restraining order to shut down fraudulent websites exploiting the COVID-19 pandemic through the sale of scarce products, such as hand sanitizer and disinfectant wipes, to consumers who never received the products.

Pandemic-related fraud schemes also pose financial risks to the Department. In a May 2020 memorandum, the OIG issued a fraud alert to warn Department procurement executives of instances in which DOJ components may have been provided substandard or mislabeled PPE, including N95 and KN95 face mask respirators. The OIG is taking appropriate actions in response to these developments. As the pandemic creates new opportunities for bad actors to target vulnerable individuals and entities, the Department's challenge is to swiftly identify, investigate, and prosecute illegal conduct.

Mitigating Health Risks While Ensuring the Rights of Individuals Subject to Immigration Court Proceedings

The Department's Executive Office for Immigration Review (EOIR) faces challenges in minimizing the health risks to all persons involved in immigration proceedings while at the same time ensuring the rights of individuals subject to those proceedings. EOIR employs approximately 520 immigration judges and over 1,200 support staff to operate its 69 immigration courts and adjudication centers nationwide. In March 2020, in response to the COVID-19 pandemic, EOIR temporarily postponed all removal hearings of non-detained individuals and individuals subject to the Department of Homeland Security's (DHS) Migrant Protection Protocols (MPP) program. Although individual immigration courts have closed intermittently for brief periods since late March, the courts have generally remained open for the performance of essential functions, including bond hearings, hearings in detained cases, and the processing of mail and filings.

Starting in mid-June, EOIR began resuming hearings in non-detained cases in select immigration courts, and as of October 23, 2020, 32 immigration courts have resumed non-detained hearings. Non-detained hearings at other immigration courts remain postponed through at least November 6, 2020. One immigration court that was closed prior to the outbreak of COVID-19 remains closed. On July 17, DOJ and DHS announced a plan to determine when to resume MPP removal hearings, though those hearings have not yet resumed as of October 2020.

In its June 2020 report identifying COVID-19 challenges for the Department, the OIG noted that EOIR has already "faced challenges in mitigating health risks for all those involved in these immigration cases," including "securing PPE for its staff and a lack of remote options to perform some work necessary to ongoing operations." Several members of Congress have

also raised concerns that EOIR's decision to resume hearings of non-detained individuals will not only impact public health and safety but also potentially threaten the fundamental fairness of immigration proceedings. The OIG is currently conducting a limited-scope review of EOIR's response to the COVID-19 pandemic to assess EOIR's communication to staff, parties to proceedings, and the public about immigration court operations; its use of PPE; its use of worksite flexibilities; and its ability to mitigate health risks while maintaining operations during the COVID-19 pandemic.

Maintaining a Safe, Secure, and Humane Prison System

Maintaining a safe, secure, and humane prison system remains a challenge for the Department and the BOP. The challenges the BOP has faced in the past—maintaining the overall safety of inmates, staff, and the public; interdicting contraband in its facilities; budget and staffing shortages; rising medical care costs due to an aging prison population; and long-term infrastructure maintenance—continue to impact the BOP. During 2020, the unexpected and unprecedented challenges presented by the COVID-19 pandemic exacerbated the strain on BOP. The First Step Act (FSA) of 2018 and the CARES Act of 2020 may help address some of these challenges, if the BOP is able to use effectively the authorities provided for by these laws.

Budget, Inmate Population Management, and Staffing Priorities

From 1980 to 2013, the total number of federal inmates grew exponentially, from 24,640 to 219,298. BOP budgets rose accordingly. In a 2013 report, the OIG noted that from FY 2001 to FY 2013, BOP's budget rose from 20 percent to 25 percent of the Department's total discretionary budget. Indeed, from FY 2000 to FY 2016, the nominal per capita cost of incarcerating an inmate in the federal system increased every fiscal year from approximately $22,000 per inmate to nearly $35,000 per inmate. Consequently, even though the BOP inmate population has declined by 29 percent from 2013 to 2020 to a current total of approximately 155,000 total inmates, the BOP continues to account for fully 24 percent of the Department's total budget request in 2020.

Two recent laws have contributed to the BOP's ability to reduce the inmate population in prison settings. The primary goals of the FSA were to improve criminal justice outcomes and reduce the size of the federal prison population while also creating mechanisms to maintain public safety. Within a year of its enactment, by January 2020, the FSA had resulted in: the release of over 3,100 federal prison inmates from BOP custody based on good conduct; 3,470 reductions of mandatory minimum sentences for crack cocaine offenses; and the expanded use of home confinement for low risk and terminally ill offenders. On March 27, 2020, the CARES Act authorized the BOP to expand home confinement authority for federal inmates if the Attorney General found that emergency conditions will materially affect the functioning of the BOP. Additionally, on March 26, 2020, and April 3, 2020, the Attorney General issued memoranda to the BOP regarding prioritizing the use of statutory authorities to grant home confinement for inmates seeking transfer in connection with the pandemic. In his April 3, 2020 memorandum, the Attorney General made the required finding that enabled the BOP to expand its home confinement authority. In response to these memoranda, on April 22, 2020, the BOP determined that it would prioritize for home confinement inmates who, in addition to meeting other basic suitability factors, either: (1) have served 50 percent or more of their sentences; or (2) have 18 months or less remaining on their sentences and have served 25 percent or more of their sentences.

As of October 14, 2020, the BOP reported that it has transferred 7,784 inmates to home confinement. Nonetheless, we have identified concerns in our inspections regarding whether the BOP fully utilized this authority at institutions that were experiencing COVID-19 outbreaks, as the Attorney General had directed. For example, we found in a July 2020 remote inspection report that despite 75 percent of the inmates at a facility within FCC Lompoc testing positive for COVID-19, as of May 13—3 months into the pandemic—only 8 inmates had been transferred to home confinement. Additional remote inspection reports of BOP facilities will similarly examine BOP's use of the CARES Act home confinement authority. In addition, the OIG is conducting a broader review of the BOP's use of home confinement as a tool to mitigate the effect of the COVID-19 pandemic on the federal prison population. This review will assess the BOP's process for implementing home confinement under the CARES Act, the process for its consideration of the eligibility criteria outlined in the Attorney General's guidance, and the process by which BOP headquarters evaluated wardens' recommendations that inmates who did not meet the Attorney General's criteria be placed in home confinement.

Despite the declining inmate population, the BOP has continued to experience significant staffing shortages for correctional officers, medical staff, and other positions. Hiring and retention remain significant obstacles. According to data provided to the OIG, the BOP had a 16 percent vacancy rate for correctional officers as of June 2020, amounting to 3,350 unfilled CO positions, and during FY 2019, BOP employees worked 6.71 million overtime hours, the equivalent of 3,107 full-time positions. These vacancies created additional challenges for the BOP as it responded to the COVID-19 pandemic. In March 2020, the BOP directed Wardens to limit the movement of staff between different areas of an institution to help control the spread of infection. However, our July 2020 remote inspection report found that FCC Lompoc officials delayed implementation of this directive for 15 days due to a preexisting shortage of correctional staff.

Medical staffing issues remain a challenge for BOP, and the challenge is particularly acute with respect to medical personnel. In January 2020, in an effort to improve healthcare recruiting and retention, the Department and OPM formally granted the BOP authority to pay physicians and dentists using the laws governing medical professional compensation in the U.S. Department of Veterans Affairs (Title 38 Pay Plan), which results in higher pay than the BOP would otherwise be able to offer. Previously only BOP psychiatrists had been approved for this pay. The BOP reported to the OIG that when it completes the required implementation steps, a total of 311 BOP psychiatrists, physicians, and dentists will be covered by the Title 38 Pay Plan. While we would expect that this action will provide important assistance to the BOP in addressing its healthcare staffing needs, more must be done to improve healthcare staffing levels, relative to the inmate population. For example, a 2020 remote inspection report found that at the Metropolitan Detention Center (MDC) Brooklyn, which houses over 1,600 inmates, shortages in medical staff resulted in the facility struggling to meet the medical needs of inmates without COVID-19 symptoms. BOP staff reported that 160 MDC Brooklyn inmate sick call requests dating to early July 2020 had not been scheduled or seen as of late September 2020. In addition, MDC Brooklyn Health Services staff indicated that both sick call requests and wait times increased significantly due to COVID 19.

Physical Safety and Security

Contraband. Contraband is a pervasive problem that requires the BOP to constantly evolve to combat new means of introduction, whether by staff or inmates. Any contraband within the prison system creates a safety risk to BOP staff, inmates, visitors, and the public.

The OIG published a report in 2016 which made 11 recommendations to the BOP to improve its ability to interdict contraband introductions. While the BOP has taken some corrective actions, 5 of the 11 recommendations remain open, including those related to revising its contraband staff search policy and upgrading its security camera system. In the 2016 report and several investigations, we found that the BOP's security camera system had serious deficiencies that adversely affected the OIG's ability to secure prosecutions of staff and inmates. The OIG determined that inmates can conceal illicit activities when they are aware of blind spots within the camera system. The BOP must expeditiously finish upgrading its security camera system to mitigate contraband introductions and other security risks.

A recent OIG audit found that the BOP faces significant and growing challenges in protecting its facilities from drone threats. Drones have been used to deliver contraband to inmates, but could also be used to surveil institutions, facilitate escape attempts, or transport explosives. In March 2020, an OIG investigation resulted in two men being charged with conspiring to use drones to smuggle contraband into Fort Dix Correctional Institute. During the investigation, the OIG obtained evidence of at least seven drone contraband deliveries at Fort Dix since July 2018.

Source: BOP

The OIG audit found that the number of reported drone incidents increased by over 50 percent from 2018 to 2019, though this data likely underestimates the full extent of the threat. We determined that the BOP needs to enhance its tracking of drone incidents to fully understand the threat. While recent legislation granted DOJ and the Department of Homeland Security additional authority to combat drone threats and the Federal Aviation Administration has approved temporary flight restrictions over 109 of the BOP's 122 federal facilities, the OIG found that delays in DOJ guidance and an absence of BOP protocol and training have hampered the BOP's efforts to safely deploy counter-drone measures. Continued coordination will be needed within DOJ and among other federal agencies to keep pace with rapidly evolving drone technology. Implementation of the OIG's recommendations will assist the Department in addressing the threat posed to BOP security by drones.

Promoting Accountability and Integrity. A significant challenge facing any prison system, including the BOP's, is promoting a culture of professionalism and integrity. A 2017 Bureau of Prisons Office of Internal Affairs report identified the most frequently sustained categories of misconduct were personnel prohibitions, unprofessional conduct, and failure to follow policy. The failure of a single staff member at an institution to follow the rules, or to comply with the law, can create serous dangers to other staff members and to inmates. OIG investigations have identified that these risks can arise across job responsibilities, from correctional officers, to healthcare workers, to Wardens and other senior managers. Indeed, a recently concluded OIG investigation resulted in the conviction of a chaplain employed by a BOP institution for smuggling Suboxone, synthetic cannabinoids, marijuana, cellular telephones, tobacco, and other contraband into the prison in exchange for bribe payments resulting in a 40-month sentence. Additionally, the OIG is investigating multiple allegations of correctional officers failing to conduct required safety checks and falsifying logs by stating that they did. For example, four correctional officers were indicted in the Eastern District of North Carolina for allegedly falsely stating that they had conducted safety checks in connection with three

unrelated inmate deaths at the FCC in Butner, North Carolina in 2019. In November 19, 2019, after the death of high-profile inmate Jeffery Epstein, two staff members were indicted for allegedly failing to conduct their required safety checks and falsifying records. Professionalism and accountability are essential foundations for staff and inmate safety.

Inmate Healthcare and Welfare

According to a 2017 Government Accountability Office (GAO) report, the BOP's obligations for healthcare rose from $978 million in FY 2009 to $1.34 billion in FY 2016, an overall increase of about 37 percent. These rising costs are largely due to an aging prison population, rising pharmaceutical prices, and increasing costs of outside medical services. As discussed in the COVID-19 Challenges for the U.S. Department of Justice report, the COVID-19 pandemic enhances the challenges of providing adequate medical care to those in custody.

The BOP faces considerable challenges due to inadequate policies, pre-planning, and contract management related to healthcare. In early 2020, the OIG found not all BOP institutions reported certain drug purchases to the BOP's Central Office, and until March 2018, the Central Office did not store or analyze historical purchase-level data. Additionally, the OIG determined the BOP did not ensure its institutions were procuring pharmaceutical drugs in the most cost-efficient ways such as effectively obtaining Big 4 pricing, a discounted government pricing available to specific agencies, or utilizing competitive bidding when required. Similarly, a 2017 GAO study determined the BOP lacks or does not analyze certain healthcare data required to understand and control its costs.

Based on recent reviews, the OIG found BOP policies do not always adequately address the needs of inmates. For example, a 2018 review reported BOP programming and policy decisions do not fully consider the needs of female inmates related to trauma treatment programming, pregnancy programming, and feminine hygiene. In 2019, a review of MDC Brooklyn facilities determined an absence of BOP policies relating to emergency preparedness led to inmates being unable to receive adequate healthcare during a power outage.

The OIG also has found that the BOP did not always provide proper administrative oversight in managing its contracts, specifically, for comprehensive medical services and mental health services. These audits identified the BOP's major weaknesses as unclear contract requirements, failure to review performance, and an inability to establish contract pricing methodology. In 2017, the OIG recommended that the BOP require comprehensive medical services contractors to submit electronic claims, ensure those claims are properly analyzed and maintained, and enforce contract language regarding fraud monitoring. Three years later, the BOP has not finished implementing these recommendations.

Infrastructure Issues

The BOP continues to encounter challenges maintaining its facilities and equipment. In its FY 2021 Budget Submission, the BOP reports that many of its facilities and much of its systems and equipment (water, sewer, electrical, and heating/air conditioning) remain aged and overused. Our recent work has revealed that BOP infrastructure issues have negatively affected the conditions of confinement for inmates. As discussed in last year's TMPC report, in September 2019 the OIG released a review and inspection in which we found that MDC Brooklyn had been aware of unresolved heating and cooling issues since at least 2014. These issues caused temperatures in certain housing units to drop below the BOP target temperature of 68 degrees on multiple occasions in winter 2019 and, at other

times, exceed 80 degrees. Since our September 2019 report, the BOP has made progress on the recommendations. However, several recommendations remain open. These include recommendations to complete heating, ventilation, and cooling equipment upgrades; take further action to diagnose and remedy temperature regulation issues if such upgrades are not effective; and ensure the use of a consistent and sound method to measure and document building temperatures.

The BOP acknowledges that failure to maintain structures can cause direct and indirect security problems. Deteriorated facilities heightened an increased risk of escape, inability to lock down cells, and potential violence due to frustration over inadequate living conditions, such as leaking and collapsing roofs. Further, as the condition of these facilities worsen, it can result in the BOP taking housing units off-line, which reduces bed space and increases system-wide crowding. As of January 2, 2020, the size of the BOP inmate population exceeded the rated capacity of its prisons by 10 to 20 percent on average, depending on the security level.

Source: BOP, with OIG enhancement

The infrastructure design of certain institutions made it difficult for the BOP to follow COVID-19 safety guidelines. For example, our July 2020 remote inspection found that FCC Lompoc's infrastructure of open bar cells rather than solid doors potentially increases the risk of COVID-19 spreading among inmates. In addition, the inspection found that inmates at one Lompoc facility were housed open dormitory style with bunk beds 3 feet apart from each other rather than the Centers for Disease Control and Prevention (CDC) guidance of 6 feet apart. In another inspection report released in July 2020, we found that FCC Tucson similarly housed inmates open dormitory style but, in contrast to FCC Lompoc, was able to increase the distance between inmates by spacing out bed assignments. In general, we found that FCC Tucson adhered to applicable COVID-19 related BOP policies and CDC guidelines and regularly communicated these changes to staff and inmates. The OIG also conducted inspections of the BOP's contract facilities. In August 2020, we issued reports in which we found that three contract facilities generally had open dormitory housing in which inmate beds are in close proximity. As noted in the pandemic section of this report, we further found that contract prisons experienced delays in receiving BOP guidance related to COVID-19. The BOP relies on contract facilities to house approximately 14,000 federal inmates. Contract prisons received most of their guidance documents between 1 and 5 days after comparable guidance was issued to BOP-managed institutions, but some delays were more significant. It is important for the BOP to ensure that contract facilities receive timely guidance so that they can take appropriate measures to contain the spread of the virus. Our inspection reports are intended to assist the BOP and the DOJ in identifying strategies to most effectively contain current and future COVID-19 outbreaks.

Recidivism

It is critical that the Department understand the changing factors that impact recidivism and develop programs designed to reduce recidivism risks.

The most recent comprehensive study by the U.S. Sentencing Commission (USSC) found that over an 8 year period, 49.3 percent of federal offenders released were rearrested; 31.7 percent of the offenders were also reconvicted, and 24.6 percent were reincarcerated. Moreover, a 2019 USSC report found that offenders who engaged in violent criminal activity recidivated at a significantly higher rate than non-violent offenders.

In December 2018, the FSA required the BOP and the Department to develop a system which, among other things, would assess the recidivism risk and criminogenic needs of all federal prisoners and place them in recidivism-reducing programs based on their specific needs. In response, the BOP created a risk assessment tool called the Prisoner Assessment Tool Targeting Estimated Risk and Need (PATTERN), in July 2019. According to a January 2020 report by the Office of the Attorney General , the Department is monitoring the use of PATTERN and will consider making future improvements and adjustments to the tool. The OIG will continue to monitor the Department's and BOP's efforts to implement the FSA.

Safeguarding National Security and Countering Domestic and International Terrorism

Enhancing national security and countering terrorism threats remain top priorities for the Department. The threats posed to the United States range from sophisticated, external plots to attacks conducted by self-radicalized lone actors influenced by foreign and domestic violent ideologies. The Department faces immense challenges in responding to such disparate threats. In addition, vigilance to the threats posed by insiders who seek to harm national security through unauthorized disclosures and theft of government secrets, and the outsiders who target our nation's most valuable secrets to gain a political, military, or economic advantage presents entirely different yet equally complex challenges.

Disrupting and Defeating Terrorist Operations

Among the Department's highest priorities are countering the threats posed by foreign and domestic terrorism. With respect to foreign terrorist organizations (FTO), the FBI remains focused on organizations such as al Qaeda and ISIS that have proven resilient despite setbacks and defeats. In February 2020, the FBI Director testified that, "In recent years, FTOs' use of the Internet and social media has enhanced their ability to disseminate terrorist propaganda and training materials to attract and influence individuals in the United States." In addition, in 2019 the FBI Director testified that, "Due to online recruitment, indoctrination, and instruction," FTOs no longer have to find ways to "get terrorist operatives into the country to carry out acts of terrorism."

Source: FBI

Domestically, the United States faces threats by both homegrown violent extremists (HVE) and domestic violent extremists (DVE). HVEs are global jihad-inspired individuals who are in the United States, have been radicalized primarily in the United States, and are not receiving individualized direction from an FTO. DVEs are individuals who seek to commit violent, criminal acts to further ideological goals stemming from domestic influences, such as those of a political, religious, social, racial, or environmental nature. The FBI believes that HVEs and DVEs currently present the "greatest" terrorist threat to the United States.

In a March 2020 OIG report, we found the FBI had not taken sufficient action to resolve certain weaknesses in its process for assessing potential HVEs and lacked comprehensive strategies to mitigate emerging challenges related to assessing potential HVEs. While the FBI conducted reviews following HVE attacks that identified the need for the FBI to improve its process for assessing counterterrorism threats and suspicious activities, we found the FBI did not ensure field offices implemented the changes and best practices recommended. Additionally, the FBI conducted an enterprise-wide evaluation of its database for tracking and managing threats and recommended additional investigative action in 6 percent of counterterrorism assessments closed between 2014 and 2016. However, we found the FBI did not ensure field

offices took appropriate action to address these investigative deficiencies. As a result, nearly 40 percent of these counterterrorism assessments went unaddressed for 18 months after deficiencies were known. We further found the FBI needs to provide adequate guidance and training to field offices to appropriately and consistently handle challenges associated with the crossover between terrorist threats and other categories of threats, such as criminal threats to life that do not have a national security nexus and threats posed by persons with mental health issues. While the FBI has made combatting HVEs one of its top priorities, more work must be done. We made seven recommendations to assist the FBI in its efforts to identify HVEs through counterterrorism assessments. The FBI's response to our recommendations will assist the Department's efforts to address this "greatest threat" to the nation. As such, the FBI has been working with the OIG since the issuance of the report to implement the necessary corrective actions to close the seven recommendations.

In another March 2020 OIG report, we found the BOP had not identified all domestic and foreign terrorist inmates in its custody and thus did not adequately monitor their communications. We found, despite BOP policy requiring staff to monitor 100-percent of the social communication such as telephone calls and emails of terrorist and other high-risk inmates, the BOP had not monitored, or had only partially monitored, thousands of such communications. In addition, we found the BOP did not take appropriate steps to ensure information about all formerly incarcerated terrorists was provided to the FBI. We made 19 recommendations to improve the BOP's accounting for, monitoring of, and security over terrorist inmates, including recommendations the BOP work with the Department to determine an accurate population of terrorists in or in transit to its institutions, establish controls that mitigate the risk of inmates communicating with unknown and un-vetted parties, and review and implement policy and procedures to ensure BOP staff are providing appropriate attention to the communications they are required to monitor. The OIG's recommendations will assist the Department in mitigating the risk of terrorists continuing their activities while in BOP custody, and the potential radicalization of other inmates by terrorist inmates engaging in prohibited activities while in custody.

In addition to the HVE threat, the FBI faces the continuing challenge of addressing threats from DVEs. According to June 2019 testimony by FBI officials before the House Oversight and Reform Committee, Subcommittee on Civil Rights and Civil Liberties, the FBI is addressing the threat posed by domestic terrorists by ensuring that every FBI field office has at least one counterterrorism squad, and some offices have a squad solely dedicated to domestic terrorism investigations. In April 2019, the FBI established the Domestic Terrorism-Hate Crimes Fusion Cell to "address the intersection of the complementary FBI missions to combat domestic terrorism and provide justice to those who are victims of hate crimes." The fusion cell facilitates information sharing across FBI divisions and positions the FBI to focus not only on current threats or recent attacks, but also to look to the future to prevent the next one.

In October 2020, the Department charged six individuals with conspiring to kidnap the Governor of Michigan, and the Michigan Attorney General charged another seven individuals with providing material support of terroristic activities. The FBI and Michigan State Police made the arrests as multiple conspirators met to pool funds for explosives and exchange tactical gear. When announcing the arrests, an FBI Assistant Special Agent in Charge stated that when extremists move into the realm of planning violent acts, "the FBI Joint Terrorism Task Force stands ready to identify, disrupt and dismantle their operations, preventing them from following through on those plans." As part of the OIG's ongoing assessment of risks in Department operations, the OIG will continue monitoring the FBI's efforts to combat domestic terrorism.

Counterintelligence and Counterespionage

Foreign intelligence services seek our nation's state and military secrets. The FBI has "observed foreign adversaries employing a wide range of nontraditional collection techniques," including using individuals who are not affiliated with intelligence services to collect information, investing in critical U.S. sectors, and infiltrating U.S. supply chains. For example, a recent U.S. Senate Permanent Subcommittee on Investigations staff report criticized the FBI for responding slowly to threats posed by Chinese "talent recruitment plans," and for lacking a coordinated national outreach program to address them. The Thousand Talents Plan, the most prominent talent recruitment plan, incentivizes individuals engaged in research and development in the United States to transmit information to China. According to the report and recent criminal prosecutions, talent recruitment plan members have downloaded sensitive electronic research files before returning to China, submitted false information when applying for grant funds, and willfully failed to disclose or lied about receiving money from the Chinese government on U.S. grant applications. The FBI Director recently described the counterintelligence and economic espionage threat from China as the "greatest long-term threat to our nation's information and intellectual property, and to our economic vitality." The Department must confront this threat by continuing to identify, investigate, and prosecute foreign adversaries and their affiliates who threaten our national security, and by providing businesses and educational institutions with the information they need to protect their own most valuable assets.

Threats to U.S. Election Security

Russia, China, Iran, and other foreign actors threaten the security of U.S. elections when they seek to interfere in the voting process or influence voter perceptions. These threats may take the form of disinformation or other social media campaigns or cyberattacks on state and local infrastructure. The Department's principal roles in combatting election interference are its counterintelligence activities in identifying, detecting, and disrupting threats to our election security, and the investigation and prosecution of federal crimes, such as violations of the Foreign Agents Registration Act and Computer Fraud and Abuse Act. According to a Deputy Assistant Attorney General of the Department's National Security Division, the Department also assists election officials, other public officials, candidates, and social media companies in "hardening their own networks, products, and platforms against malign foreign influence operations." In FBI Director Wray's written remarks on September 17, 2020, before the House Homeland Security Committee he stated, "Our nation is confronting multi-faceted foreign threats seeking to both influence our national policies and public opinion and cause harm to our national dialogue. The FBI and our interagency partners remain concerned about, and focused on, the covert and overt influence measures used by certain adversaries in their attempts to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine the American people's confidence in our democratic processes." Furthermore, the Directors of the FBI, National Security Agency, Cybersecurity and Infrastructure Security Agency, and National Counterintelligence and Security Center issued a joint message on October 6, 2020, discussing their agencies' commitment and methods to protect and ensure the integrity of the 2020 election.

As noted in the October 2019 Volume II of the bipartisan Senate Select Committee on Intelligence (SSCI) Report on Russian Active Measures Campaign and Interference in the 2016 U.S. Election, in 2016 Russian operatives masqueraded as Americans and "used targeted advertisements, intentionally falsified news articles, self-generated content, and social media platform tools to interact with and attempt to deceive tens of millions of social media users

in the United States." Although the Committee found that the U.S. intelligence community's ability to identify and combat foreign influence operations carried out via social media channels has improved since the 2016 U.S. presidential election, it cautioned that detecting foreign influence operations on social media becomes more difficult as the underlying enabling technology continues to advance. As a result, one of the most significant challenges for the Department is detecting and disrupting these evolving threats to our election security, in order to preserve the integrity of our elections and the will of the American people.

Combatting Insider Threats and Unauthorized Disclosures


Source: FBI

In accordance with its 2018-2022 Strategic Plan, the Department must continue to protect itself against insider threats and potential leaks of sensitive information. The Department recently has prosecuted insiders who allegedly made unauthorized disclosures of sensitive information. These insiders have included a Defense Intelligence Agency counterterrorism analyst who pleaded guilty in connection with charges that he provided classified national defense information to two members of the news media, and a former federal government employee and contractor who pleaded guilty in connection with charges that she improperly retained a classified document that outlined intelligence information. The Department has also prosecuted government insiders, including former CIA officers, for sharing or attempting to share information with our foreign adversaries as part of our adversaries' espionage and intelligence-gathering efforts.

In addition, the Department should maintain a high level of vigilance to mitigate the insider threat risk. Among other things, it should examine its controls over employee and contractor access to sensitive information, limit such access to those required to have it, and ensure that it continuously monitors and updates the list of persons with authorized access. In 2017, the OIG issued a report on its audit of the FBI's insider threat program. We made eight recommendations to improve the FBI's program for deterring, detecting and mitigating malicious insider threats, including recommendations that the FBI ensure insider threat leads are handled and monitored in a systematic way, and that all classified systems and networks have user activity monitoring coverage. The FBI concurred with all of our recommendations. More recently, the OIG initiated an audit that will assess the FBI's internal controls related to the physical security of covert video and audio equipment and data under a contract awarded by the FBI to a third party.

To protect itself, and the nation's security, from insider threats, the Department must promote and cultivate an internal culture that values the security of sensitive information, and the confidentiality obligation that all Department employees have.

Protecting the Nation and Department Against Cyber-Related Threats and Emerging Technologies

Cyber-related threats have the potential to adversely impact the national security and the domestic economy. As both a law enforcement agency and a member of the Intelligence Community, the Department has an integral role in protecting the nation against these threats. Moreover, as a repository of classified national security information, law enforcement sensitive information, and other sensitive but unclassified information, the Department must ensure that its own information systems are secure in the face of cyber-related threats.

Responding to Known, Evolving, and Novel Threats

Adversaries of the United States utilize cyber technologies to advance their political, military, and economic interests. In July 2020, the Director of the U.S. National Counterintelligence and Security Center (NCSC) warned in connection with the 2020 national election that malicious cyber actors are trying to gain access to U.S. state and federal networks, including those responsible for managing elections. Moreover, the NCSC Director identified China, Russia, and Iran as adversaries who seek to harm our electoral process. Similarly, the Director of National Intelligence testified in 2019 that hostile states and actors including China and Russia are "intensifying online efforts to influence and interfere with elections" in the United States and abroad. Further, the Senate Committee on Intelligence investigated Russian interference in the 2016 national election and found in a July 2019 bipartisan report that Russia attempted to influence and undermine the U.S. electoral process.

Source: FBI

Although the Department continues to dismantle cyber-enabled terrorist financing campaigns, initiate criminal investigations into individuals who have conducted cyberattacks on private companies and citizens, and prosecute perpetrators of ransomware attacks against local municipalities and public institutions, many critical cyber threats remain.[1] These threats include cyber scams against individuals, such as ransomware attacks and extortion through social media accounts, theft of trade secrets, and cyberstalking. Additionally, according to the FBI, terrorist and criminal organizations are using sophisticated cyber tools including cryptocurrency and social-media-based fundraising to finance their operations. As cyber technologies and the manner in which they are employed evolve quickly, the Department's challenge is to coordinate closely with other government agencies on strategies to anticipate novel cyber threats, while continuing its successful efforts to thwart known methods of attack.

An important response strategy to mitigate cyberattacks ensures victims are notified of cyber intrusions. In 2019, the OIG reviewed the FBI's Cyber Victim Notification process and identified issues with the completeness and reliability of the data stored in the FBI's data system. These issues rendered the FBI unable to determine if all victims were notified of

1 Ransomware is a type of malicious software, or malware, which prevents computer users from accessing computer files, systems, or networks and demands the payment of a ransom for their return.

cyber intrusions and impaired the ability of victims or potential victims to mitigate threats to their systems. The FBI agreed with the OIG's recommendations to close this information gap to address victim vulnerability.

Emerging technologies, such as unmanned aircraft systems (UAS) and three-dimensional printed firearms, present new challenges to the Department. UAS-commonly referred to as drones-have become more powerful and easier to pilot, and, as such, the Attorney General has noted, "they have also become a more attractive tool for criminals, terrorists, and other bad actors to cause disruption and destruction." To assist the Department in addressing its challenges related to emerging technologically-related threats, the OIG issued a report in September 2020 on the Department's efforts to protect BOP facilities against threats posed by UAS, including contraband delivered to BOP facilities by drones and other security threats posed by drones. We found the BOP faces significant and growing challenges to protect its facilities from drone threats and needs to improve its tracking of drone incidents, improve its drone response guidance, and collaborate with the Department and other federal agencies to identify and obtain technologies suitable to secure BOP facilities from drone threats. We made seven recommendations to improve the BOP's tracking of drone incidents and promote efforts to protect its facilities against drone threats. The threat posed by drones to BOP institutions is discussed further in the Prisons section of this report.

Three-dimensional (3-D) printing of firearms represents another emerging technology trend with implications for public safety. The OIG is auditing the ATF's oversight of 3-D firearm printing technology. Our preliminary objective is to evaluate the effectiveness of ATF policies and procedures regarding the regulation and oversight of 3-D firearms technology and trafficking. The OIG expects to provide recommendations during FY 2021 to assist the Department in addressing the challenges presented by this emerging technology.

Challenges Investigating and Prosecuting Cyber-related Crime

Encryption and Lawful Access. Impenetrable device encryption can prevent law enforcement from searching for or accessing evidence on devices that have been lawfully-seized, and end-to-end encryption can interfere with the Department's ability to effectively conduct wiretaps of individuals who are suspected of planning or engaging in criminal activity.[2] According to the Attorney General's Cyber Digital Task Force (Cyber Digital Task Force), encryption can limit the Department's access to critical evidence and hinder its efforts to investigate a wide variety of criminal activities, including violent crime, drug trafficking, child exploitation, money laundering, and domestic and international terrorism. Additionally, according to the Cyber Digital Task Force, many communications service providers are not retaining the means to access encrypted data even if necessary to comply with a search warrant or court order.

To overcome the challenge that encryption poses, the Department is continuing to engage with technical experts and explore and utilize other options for accessing encrypted data and devices, such as by lawfully exploiting software vulnerabilities. However, such methods may be expensive, time-consuming, and not universally applicable. For example, it took FBI technical experts over four months to gain access to significant evidence stored on two Apple iPhones belonging to Mohammed Saeed Alshamrani, the perpetrator of the December 6, 2019 shooting at Naval Air Station Pensacola that killed three U.S. sailors and severely wounded

2 Devices with end-to-end encryption, also known as warrant-proof encryption, can be timely decrypted only by the end user or customer.

eight other Americans—even though the court authorized the FBI to search the iPhones within one day of the shooting. In a March 2018 OIG report, we examined the circumstances under which the FBI, assisted by a third party, was able to access the data of an iPhone of Syed Rizwan Farook, one of the subjects believed to have been responsible for the December 2, 2015 terror attack in San Bernardino, California. We found that inadequate communication and coordination caused a delay in engaging all relevant personnel from the FBI's Operational Technology Division (OTD), as well as the outside party that ultimately developed the method that unlocked the phone, in the search for a technical solution to the Farook iPhone problem. The FBI took steps to address these issues before the publication of our report. We recommended that the FBI take the remaining necessary steps to improve coordination between the FBI units that work on computer and mobile devices.

The Department has also monitored and explored potential legislation that seeks to address the lawful access problem by, for example, imposing lawful access assistance requirements on certain defined classes of major communications and device operating system providers.

The Dark Web. The "dark web," or Darknet, is a part of the Internet that cannot be accessed through standard web browsers and allows individuals to hide their identity and location. According to the Cyber Digital Task Force, criminals regularly use the dark web to facilitate many types of criminal activity, including narcotics and arms trafficking, identity theft, and the sexual exploitation of children. The investigation and prosecution of criminal activity conducted on the dark web continues to be a significant challenge for the Department.

Despite this ongoing challenge, the Department has had some recent success disrupting illegal dark web activities. For example, in September 2020, the Department, through the Joint Criminal Opioid and Darknet Enforcement (JCODE) team, joined Europol to announce the results of Operation DisrupTor, a coordinated international effort to disrupt opioid trafficking on the Darknet. According to the Department, Operation DisrupTor resulted in the arrest of 179 Darknet drug traffickers and criminals who engaged in tens of thousands of sales of illicit goods and services across the United States and Europe. In October 2019, the Department announced the indictment of a South Korean national for his operation of Welcome To Video, a child sexual exploitation marketplace on the dark web; the takedown of the site; and the arrests of and charges filed against 337 site users. The Department credited the law enforcement operation, conducted by the Department and other U.S. and international law enforcement agencies, for the rescue of at least 23 minor victims who were being actively abused by the users of the Welcome To Video site.

Source: DOD

The OIG recently completed an audit that covered numerous aspects of certain DEA undercover investigative activity and found that the DEA's management of undercover money laundering investigations involving virtual currency on the dark web was insufficient due to inadequate headquarters management, lack of policies, inadequate internal control procedures, insufficient supervisory oversight, and lack of training. As the Department expands its traditional investigations to target dark web activities, the Department's challenge is to ensure that it has proper procedures and oversight in place.

The OIG is currently auditing the FBI's strategy and efforts to disrupt illegal dark web activities. The preliminary objective of our work is to assess the implementation of the FBI's dark web strategy. The OIG expects to provide recommendations to the FBI early in FY 2021 to assist the Department in improving its investigative and planning efforts related to the dark web, and developing a coordinated FBI-wide dark web approach.

Strengthening the Department's Capabilities and Defenses

The critical work of the Department involves the collection and use of a large volume of classified, law enforcement sensitive, and privacy protected information. The Department must ensure that its data systems and information handling protocols are appropriately secure to protect such information. 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 2019, in addition to assessing the information security programs of the Tax Division and each component identified below, the OIG assessed the following component-specific systems: FBI's Enterprise Application Service Program, Land Mobile Radio Network, and Legacy Pocatello Data Center; the International Criminal Police Organization (INTERPOL) Washington, U.S. National Central Bureau's OA/Envoy System; the Justice Management Division's (JMD) Personnel Accountability and Assessment System; OJP's Denial of Federal Benefits and Defense Procurement Fraud Debarment Clearinghouse System (DFB/DPFD); the Tax Division's Office Automation System; and the BOP's Sentry System. We found deficiencies in the IT security of each component whose information system we assessed, and we made recommendations for improving each component's information security program. We also identified at least one weakness in each of the following: the FBI's Legacy Pocatello Data Center, the BOP's Sentry System, and the OJP's DFB/DPFD System. The Department's attention to the issues we identified and recommendations we made is important to preserving the Department's information security and protecting Department information from cyber-related threats.

In addition, during criminal and administrative investigations, the OIG found systemic concerns with the BOP's compliance with cyber security and related issues. Based on these concerns, the OIG issued a MAM to the BOP regarding the practice of allowing personnel to have a "personal container" on their government-issued phones without properly training the personnel on appropriate uses of the container. In addition, the OIG identified non-compliance by the former FBI Director with Department policies regarding use of personal devices to conduct official Department business. These practices pose security risks and undermine the Department's ability to maintain appropriate security over the sensitive information it regularly processes. The Department should take steps, consistent with the OIG's recommendations, to ensure better adherence to computer rules of behavior to enhance the security of information processed on Department systems.

The Opioid Crisis, Violent Crime, and the Need for Strong Law Enforcement Coordination

The past year has seen progress and setbacks in the areas of the opioid epidemic and violent crime. While nationwide violent crime declined in 2018 and the first 6 months of 2019, FBI statistics reflect a 15 percent increase nationally, between 2019 and 2020. The opioid epidemic has been complicated by the COVID-19 pandemic during 2020. After drug overdose deaths declined for the first time in 25 years in 2018, they rose again in 2019, and are currently on track to rise substantially in 2020. Critical to addressing these two enforcement and community priorities is coordination among law enforcement agencies. As the nation's leading law enforcement agency and supporter of local law enforcement efforts, this is one of the significant challenges that the Department continues to face.

Law Enforcement Coordination and Information Sharing

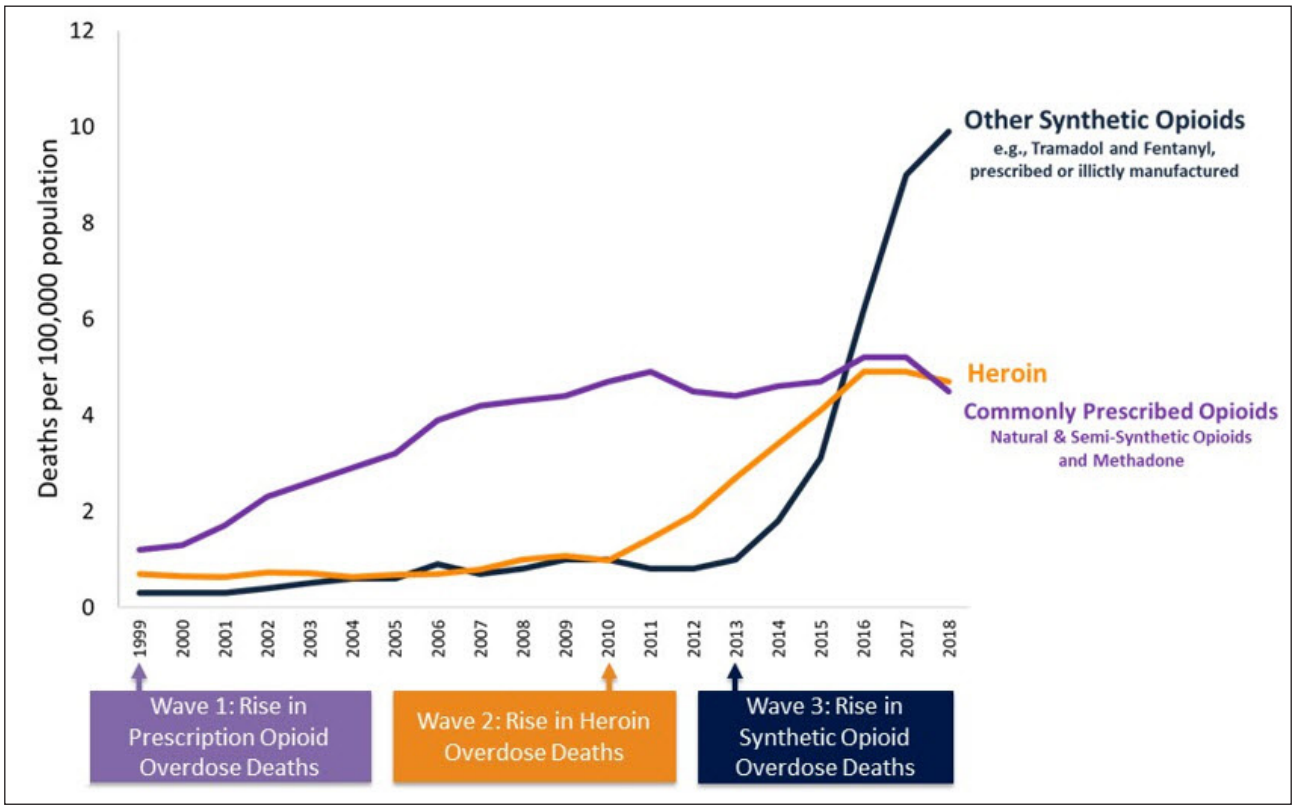
Information sharing among federal agencies is an ongoing challenge. For example, as noted in the OIG's FY 2019 TMPC Report, a July 2019 joint DOJ and Department of Homeland Security OIG review of law enforcement cooperation on the Southwest border found a lack of information sharing policies between the FBI and Homeland Security Investigations (HSI), resulting in over one-third of special agent survey respondents reporting at least one cooperation failure between agencies, a range of deconfliction and information sharing issues that required attention, special agents lacking an understanding of the other agency's mission and authorities, and many agents lacking trust in the other agency or its personnel. This review made five recommendations to improve cooperation between the FBI and HSI. Further indicative of the lack of coordination between these two federal agencies is that more than a year after issuance of the joint report, the key recommendation, requiring a memorandum of understanding between FBI and HSI on information sharing and coordination, remains open. Although the FBI has agreed with the recommendation, HSI has not concurred.

Combatting violence and hate crimes requires the effective collection and sharing of detailed information among federal, state, local, and tribal law enforcement agencies. According to OJP, since the 1970s, the OJP's Regional Information Sharing Systems (RISS) Grant Program has fully funded 6 regional networks that connect more than 9,400 local, state, federal, and tribal law enforcement and public safety agencies. The RISS program awarded a total of nearly $29 million in 2019. RISS coordinates the sharing of law enforcement sensitive information and intelligence, deconfliction notifications, and investigative data. In September 2019 and August 2020 audits, the OIG identified grant funds being used for unallowable purchases, including to pay professional dues to the RISS Director's Association (RDA). In November 2019, we issued a MAM recommending that OJP consider requiring RISS Centers to stop funding the RDA because the RDA used those funds for gifts and payments to an organization that provides lobbying services. This unallowable use of grant funds shows the need for enhanced internal controls with the RISS program and reflects the challenge of facilitating coordination and information sharing, which are essential parts of the law enforcement mission.

The Opioid Crisis

After rising every year for 25 consecutive years, drug overdoses declined slightly in 2018, only to increase by 4.8 percent in 2019, and set a new record high of nearly 73,000 deaths in the 12-month period ending in February 2020. Although the DEA initially reduced the annual quota for opioids in 2020, the public health emergency of the coronavirus pandemic led to a reversal of this decision, as well as other policy changes that were intended to ensure availability of opioids for ventilator patients stricken with COVID-19 and other patients who suddenly lacked direct access to doctors and clinics. A May 13, 2020 report by the Office of National Drug Control Policy shows an 11.4 percent year-over-year increase in fatalities for the first 4 months of 2020, and an increase of 18.6 percent for non-fatal overdoses during that time frame. If the current trend of overdose deaths continues through 2020, it will be the sharpest annual increase since 2016, when the synthetic opioid, fentanyl, first made significant inroads into the country.

3 Waves of the Rise in Opioid Overdose Deaths



Source: CDC National Vital Statistics System Mortality File

The Department currently participates in many initiatives including 15 health care fraud strike forces in 24 districts. According to a joint statement from the Department's Director of Opioid Enforcement and Prevention Efforts and the Assistant Administrator of the DEA's Diversion Control Division, these task forces conducted over 1,300 investigations in 2018 and charged over 300 doctors with health care fraud involving opioids, a 52 percent increase from the previous fiscal year.

The OIG has recently issued three reports relating to the continuing efforts to address the opioid epidemic. The reports found that the DEA had made progress in key areas, such as forming partnership with state and local counterparts and allowing the public to safely

dispose of unwanted pharmaceuticals; however, these reports also identify a number of areas where additional efforts and improvements could be made, such as outcome-based performance strategy and data analysis to minimize coverage gaps. DEA's effort to close the OIG's recommendations in these reports, described below, will assist the Department in its continued efforts to address the ongoing challenges presented by opioids.

In a 2019 report, the OIG made several findings and recommendations relating to the DEA's strategy to address the diversion of opioids from permissible to illegal purposes. The OIG report cited, among other things, failures of the DEA's preregistration process to adequately vet all new applicants and policy shortcomings which allowed individuals whose registration had been revoked or surrendered to reapply for registration the day after losing their registration. In the past year, the DEA has taken positive actions relating to these recommendations. For example, on October 23, 2019, the DEA launched a new centralized database for distributors to make Suspicious Order reports, along with other regulatory improvements that will better allow the DEA to identify and investigate registrants who violate the Controlled Substances Act. Further, the DEA reopened an interim final rule which allows practitioners to write prescriptions for controlled substances electronically. However, the DEA still has work to do in connection with the OIG's 2019 report, including taking steps to ensure that DEA diversion control personnel responsible for adjudicating registrant reapplications are fully informed of the applicants' history and are implementing electronic prescribing safeguards to combat prescription fraud.

In September 2020, the OIG issued a report on the DEA's community-based efforts to combat the opioid crisis. Since 2016, the DEA has deployed in 20 "pilot cities" its "360 Strategy," which brings together U.S. Attorney's Offices, state and local law enforcement, educators, prevention and treatment providers, and other entities to reduce the impact of opioid misuse and addiction. Taking these actions to enhance coordination with their state and local counterparts, as well as health care professionals, was an important step forward by the DEA. The OIG report found, however, that despite multiple oversight efforts, the DEA still lacks an outcome-oriented performance measurement strategy to assess the effectiveness of its 360 Strategy. Consequently, the OIG recommended that the DEA develop clearly defined goals prior to project implementation and include a focus on sustainability. We further recommended that the DEA enhance its pilot city selection process by supplementing its use of CDC data with broader information. For example, we found that the DEA should review field data on fentanyl from an availability and seizure standpoint, since most current data shows that fentanyl causes about as many U.S. deaths as prescription opioids and heroin combined. In addition, the DEA should enhance its efforts to both increase awareness of treatment options and correct misconceptions related to its position on medication-assisted treatment. We also found that the DEA should strengthen its collaboration with other Department components, including OJP, which grants nearly half a billion dollars to combat the opioid crisis, and the COPS Office, which can enhance the DEA's opioid-related efforts from a law enforcement perspective.

In September 2020, the OIG also released a report on the DEA's National Drug "Take Back" Initiative (NTBI). Since 2010, the DEA has held the NTBI to provide easy, anonymous opportunities to remove medicines in the home—including unused, expired, or unwanted prescription drugs—that are highly susceptible to misuse, abuse, and theft. This audit found that since 2010, the NTBI has successfully facilitated the collection and destruction of over 12 million pounds of unwanted and potentially dangerous pharmaceuticals. As part of these efforts, the OIG recommended that the DEA perform regular analysis of Take

Back Day activities, in conjunction with available data from within the DEA or external sources, to identify strategies for expanding Take Back Day participation by state and local counterparts, minimize coverage gaps, and better inform the public of all prescription drug disposal options. Through such analysis, the DEA can better target its efforts to increase law enforcement agency participation and community awareness. For example, the OIG found that the DEA could identify locations that would benefit most from the Take Back Day Program by using existing data on where prescription drug diversion and opioid use presents the greatest challenge.

Source: DEA

Source: DEA

The OIG is also conducting ongoing work related to the Department's response to the opioid crisis. In December 2019, the Department announced awards of more than $333 million to help communities affected by the opioid crisis, ranging from drug courts to a comprehensive program for opioid abuse, called the Comprehensive Opioid, Stimulant, and Substance Abuse Program (COSSAP). Recently, OIG initiated an audit of the COSSAP to assess the oversight and management of the program, thereby further assisting the Department's efforts in this area.

The opioid epidemic is not only a critical public health issue facing the nation, but also a significant challenge of public safety for the Department. The OIG will continue to conduct rigorous oversight to ensure that the Department adequately addresses this crisis.

Violent Crime

Ensuring the safety of our communities by reducing violent crime continues to be a critical challenge for the Department. While the U.S. violent crime rate is nearly half of what it was at the 1992 peak, violence remains a persistent problem for many communities. Between 2014 and 2016, homicides increased 20 percent, the highest rate of increase in 49 years. Since then, the Department's FY 2019 Performance Report indicated that it achieved 11 of its 13 FY 2019 targets for reducing violent crime and promoting public safety. However, in 2020, there has been a substantial increase in violence in many cities. Additionally, the FBI reports that hate crimes against minority groups continue to rise. Indeed, the FBI Director has testified that the "top threat we face from domestic violent extremists stems from those we identify as racially/ethnically motivated violent extremists." The pandemic has heightened these concerns and prompted legislation to be introduced in Congress to combat COVID-19 hate crimes. As always, the challenge is to focus the most effective law enforcement efforts and violence reduction programs in the areas that need them most.

The Department identified the reduction of violent crime as a goal in its 2018-2022 Strategic Plan. The Department's strategies for accomplishing this goal include activities intended to: (1) support, train, and work in partnership with state, local, and tribal partners to make communities safer; (2) dismantle violent transnational criminal organizations and gangs; (3) protect victims of crime from exploitation and revictimization; and (4) identify, arrest and prosecute violent criminals for gun violence and other violent crimes.

In FY 2020, the Department launched Operation Relentless Pursuit, an initiative aimed at combatting violent crime, through a surge of federal resources, in seven cities experiencing increasing levels of violence. Subsequently, in July 2020, the Department initiated Operation Legend, which sought to also involve state and local law enforcement officials in this effort. Since the latter operation's launch, through August 31, 2020, more than 2,000 arrests have been made, including 147 for homicide.

The OIG is currently reviewing the Department's strategic plan and accountability measures for combatting violent crime, including coordination across Department prosecution, law enforcement, and grant-making components. This review will also assess the Department's strategic plan for providing assistance to communities that are confronting significant increases in homicides and gun violence.

Regarding the Department's efforts to combat international crime, the OIG is conducting an audit of the DEA's establishment and oversight of DEA-supported foreign law enforcement units as part of its ongoing efforts to dismantle violent transnational criminal organizations and gangs. Among other things, the audit will evaluate the DEA's process for establishing DEA-supported law enforcement units abroad, including Sensitive Investigative and Protective Police Units.

As the Department continues to confront rising violent crime, as well as the ongoing national opioid epidemic, the OIG will focus its oversight on the effectiveness of the Department's efforts in these critical areas.

Ensuring Financial Accountability of Department Contracts and Grants

In FY 2019 the Department awarded approximately $8.5 billion in contracts and over $4.9 billion in grants. The passage of the CARES Act in March 2020 provided $1 billion in funding to the DOJ for addressing the COVID-19 pandemic, of which $850 million is being administered by OJP. Oversight of all contracts and grants awarded to ensure financial accountability and mitigate the risks of fraud or misuse of contract and grant funds is an ongoing challenge. The Department faces an added challenge in connection with the CARES Act awards because of the urgent need to have made the awards promptly.

Contracts Oversight

Compliance with the FAR. The Federal Acquisition Regulation (FAR) is a complex set of rules, and the DOJ continues to face challenges administering and overseeing its contracts in compliance with the FAR. As discussed in last year's TMPC report, multiple OIG contract audits consistently identified FAR-related noncompliance.

Frequent Findings in OIG Contract Audits included in July 2020 Management Advisory Memorandum:

- **Inadequate execution of contract oversight responsibilities**
- **Insufficient quality assurance practices**
- **Non-compliance with contract-related laws and regulations**

In FY 2020, we have continued to find compliance issues with the FAR in contract audits. For instance, in June 2020, we issued an audit report of the ATF's administration of its sole-source contracts to a vendor for criminal gun intelligence services in support of the National Integrated Ballistic Information Network. This audit found that ATF did not ensure appropriate oversight of contractor performance, and did not include required whistleblower protection clauses in the contracts. Persistent findings from contract audit reports over time suggest a pattern of systemic weakness in contract administration and FAR compliance that the DOJ must address.

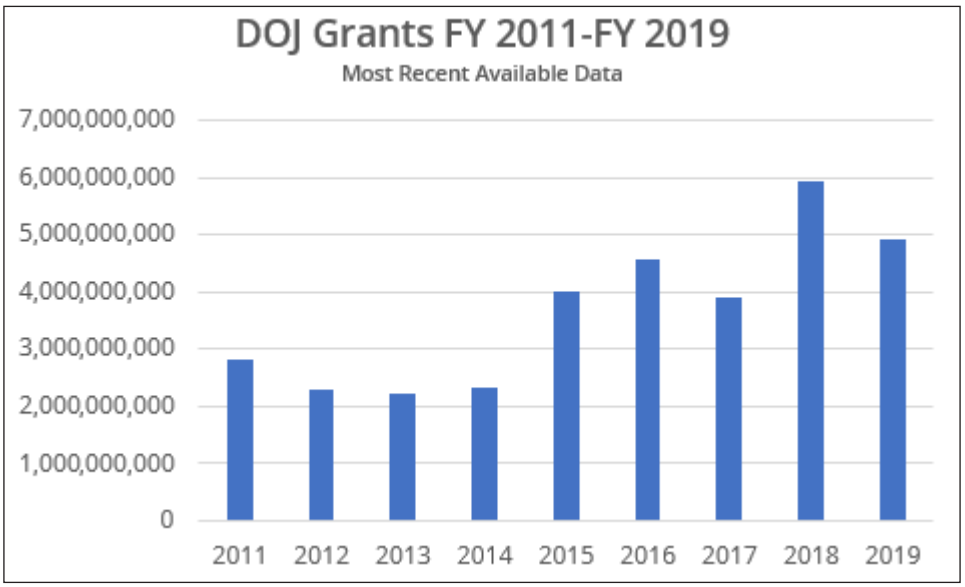
To assist the Department in improving its adherence to the FAR and its contract oversight, in July 2020, the OIG issued a MAM to the JMD. Our MAM identified the recurring, potentially systemic issues from our reports and summarized our findings and recommendations. Specifically, among other things, our MAM reported that from FY 2013 through FY 2019, the DOJ awarded over $54 billion in contracts for products and services. Over those same 7 years, OIG audits of the DOJ's contracts have frequently found noncompliance with the FAR due to inadequate execution of contract oversight responsibilities; insufficient quality assurance practices; and failure to maintain documentation to support procurements, maximizing competition, and avoiding personal services contracts. This MAM recommended that the JMD consider including contract management in its enterprise-level risk management prioritization. We further recommended that the JMD ensure components update their contractor-related monitoring policies, as well as develop policies and procedures for

proper training of contract Task Monitors and accurate and timely submission of contractor performance evaluations to the Contract Performance Assessment Reporting System. JMD agreed with all four recommendations. The Department can improve its oversight of the significant monies awarded through contracts by implementing these OIG recommendations.

Procurement Issues at the BOP. In addition to contract audits, OIG investigations have led to the issuance of a MAM to the BOP in spring 2020 over concerns of how it procures food products, which accounted for 5.7 percent or $401 million of its FY 2019 budget. Specifically, a series of recent OIG investigations found that the BOP does not have a quality assurance plan to ensure that food products procured by the BOP meet the specifications outlined in contracts. As a result of our investigations, two individuals pleaded guilty in 2019 to charges related to providing $1 million of adulterated meat of more than 775,000 pounds to 32 BOP institutions. More recently, our investigation led to three companies and two individuals being debarred in August 2020 for 3 years by the DOJ's Debarment Official for knowingly providing adulterated food products in connection with over $500,000 in contract awards. In our MAM, the OIG made 3 recommendations to the BOP to enhance its procurement practices on pre-award diligence, contractor performance, and quality controls. These recommendations are designed to help BOP reduce the risks of fraud and inadequate contractor performance.

Grants Oversight

The graph below shows the amount of funds awarded in grants by DOJ components since FY 2011, which as the chart reflects grew substantially in FY 2015. The reason for the increase is that Congress more than tripled the annual amount of Crime Victim Funds (CVF) available from the previous year to enhance the provision of victim services through grants awarded by OJP. Since that same year, the OIG has received $10 million each year to provide oversight of this enhanced CVF funding.



Source: OIG analysis of data from OJP, Office on Violence Against Women and the COPS Office

Adequate controls over the administration and management of grant funds present a continuing challenge for the DOJ and increase the risk of fraud. Specific areas of concern include the CVF, OJP methodology of addressing dollar-related recommendations, and non-

CVF grant program issues. The current public health crisis has heightened these concerns after the DOJ received dedicated grant funding from the CARES Act to address the pandemic.

Pandemic Grant Funds. In addition to managing existing grant programs and awarded contracts, the DOJ must also implement adequate controls on funding from the CARES Act. The infusion of funds that resulted from the pandemic has increased the potential of fraud and misuse of public resources, as we have alerted the DOJ procurement executives in a May 2020 memorandum. In the pandemic section of this TMPC report, we discuss our interim report on OJP's implementation of CARES Act grant funds and our finding that the OJP has awarded Coronavirus Emergency Supplemental Funding (CESF) grants in a timely manner based on our ongoing review. For the OJP and the Department, the additional challenges following the grant awards are ensuring that award recipients use the funds to address the pandemic and mitigating the risk of potential misuse of the monies.

CVF: Audits and Outreach Efforts. In recent years, our TMPC reports have discussed challenges of administering and overseeing CVF grants due to the significant increase of available funds since FY 2015. Established by the Victims of Crime Act (VOCA) of 1984, the CVF collects criminal fines and penalties which it then distributes annually to all states and most territories to support victim services. From January 2016 to the present, we have issued more than 70 CVF-related audit reports, including two comprehensive audits issued in 2017 and 2019 on OJP's efforts in managing the CVF. These two comprehensive audit reports found CVF grant recipients struggling with monitoring thousands of subrecipients, as well as some complex and ambiguous criteria. OJP agreed with the 25 recommendations in these two reports on improving its administration of the CVF, and has made significant improvements to address these recommendations by issuing written guidance to clarify reporting discrepancies and offering financial management training to the states and subrecipients.

We also conducted outreach in 2019 and 2020 by co-presenting with the Department's Office for Victims of Crime at the annual training conference of the National Association of VOCA Assistance Administrators. At these conferences, attended by CVF grant awardees, we discussed audit procedures and insights from the more than 200 recommendations in our CVF audit reports to highlight best practices for the grantees, and how they could avoid common pitfalls. While we believe these outreach efforts will enhance compliance with the grant rules, we continue to identify issues of concern in our recent CVF audits. Although these state grantees enhanced their programs serving crime victims, we identified inadequate financial controls, such as inaccurate calculations on state certification forms and ineffective policies to detect unallowable and unsupported expenditures. Closing the OIG's recommendations in connection with CVF awards will greatly assist the Department in its oversight of the substantial funds it receives to award for crime victim services.

Corrective Actions on Audit Recommendations. Federal guidance requires auditees to respond to OIG audit recommendations, including completed or planned courses of action in response to recommendations, and timeframes for final resolution. In March 2020, the OIG issued an audit report that examined OJP's review of corrective actions for dollar-related recommendations issued by the OIG regarding DOJ grant recipients. The OIG found that OJP remedied these recommendations often by issuing retroactive approvals for costs that we had determined were unallowable by the terms of OJP's grants at the time of the audit, or accepting supporting documentation not made available by grantees to the OIG during the audit. The average timeframe for closing all recommendations in a report for our review scope was over 3 years. OJP agreed with the OIG's three recommendations in this report

to enhance its review of post-audit corrective actions by grant recipients. By addressing our audit recommendations with grant recipients in a timelier manner, the Department can ensure better contemporaneous accountability by the grantees for their use of funds, and enhance the overall quality of its grant oversight efforts.

Grant Monitoring: Safety-Issues and Reliable Metrics. Another challenge that the Department has faced is programmatic concerns in grant programs. For instance, in last year's TMPC report we discussed two 2019 audits that identified problems in grant programs that provided programming for the benefit of minors—one report related to DOJ's youth-centered grant programs and the other report related to a school district grant recipient. While the DOJ works towards implementing recommendations of those audit reports, we have continued to find programmatic concerns in recent grant audits. In May 2020, the OIG issued an audit report of two OJP cooperative agreements from the Comprehensive Services for Victims of Human Trafficking program to a non-profit. The audit found that the grant recipient did not comply with a special condition on submitting policies and procedures on maintaining confidentiality of victims' names, addresses, telephone numbers, or any other identifying information, within 90 days of the award. In March 2020, the OIG issued an audit report of four cooperative agreements from the same program to another non-profit recipient. Although we did not identify the same safety concerns as the previous example, we found that all progress performance reports we reviewed had inaccurate or unsupported metrics on outreach, training, and trafficking victim referrals. The DOJ must strengthen the implementation of its grant programs to ensure that resources accomplish its goals through reliable metrics and without harming participants.

Strategic Planning: The Department's Challenges to Achieve Performance-Based Management and to Enhance Human Capital

Pursuant to the Government Performance and Results Modernization Act of 2010 (GPRA Modernization Act), the Attorney General established four strategic goals in the DOJ FY 2018-2022 Strategic Plan. One of these goals encompasses promotion of "good government," which has as its objectives the achievement of management excellence, workforce development, and deployment of innovative technology.

In July 2016, the Office of Management and the Budget (OMB) issued Circular A-123 which stated, "Over the years, government operations have changed dramatically, becoming increasingly complex and driven by changes in technology. At the same time, resources are constrained, and stakeholders expect greater program integrity, efficiency and transparency." Accordingly, Circular A-123 made policy changes requiring agencies to implement an Enterprise Risk Management (ERM) capability coordinated with the strategic planning and strategic review process established by the GPRA Modernization Act, and the internal control processes required by Federal Manager's Financial Integrity Act (FMFIA) and GAO's Green Book. This "integrated governance structure" is intended to "improve mission delivery." Consequently, Department leaders are faced with challenges in their mission-driven efforts to (1) achieve performance-based management and (2) to enhance its human capital according to the current DOJ Strategic Plan, which entails producing accurate information and developing the workforce as described below.

The Department's Challenge to Achieve Performance-Based Management

Performance-based management involves using reliable statistics and narratives to ensure programs are achieving set goals and contributing to the overall mission of the Department. Despite the critical nature of utilizing performance data, many Department components lack either meaningful performance measures or the data necessary to evaluate their programs. For example, the Department has identified disrupting and dismantling drug trafficking organizations to curb opioid and other illicit drug use in our nation as one of its measured objectives. Within this objective, the DEA is tasked with submitting certain data to the Department, such as the number of opioid prescriptions and diversion cases completed. However, in a September 2019 report, the OIG found that DEA did not use its available resources, including its data systems, to detect and regulate diversion effectively. Further, in a September 2020 report, the OIG found that between 2016 and 2019, the DEA deployed its 360 Strategy in 20 communities across the U.S., where it has helped to increase awareness of opioid-related issues, provide training, build anti-drug coalitions, and create online resources available to the public at no charge. While these are positive strides, the OIG found that the DEA needs to improve performance metrics to assess the value and effectiveness of the community-based efforts undertaken as part of its 360 strategy. We similarly found in a June 2020 review that although the DEA identified certain undercover operations as one of its most successful tools, the DEA did not track operational achievements in a way that allowed DEA management, the Department, or Congress to understand whether operations successfully completed the authorized objectives and goals, built cases that

led to prosecutions, and deprived criminals of ill-gotten gains. We also found that the DEA did not always leverage information or strategically evaluate connections between these undercover operations.

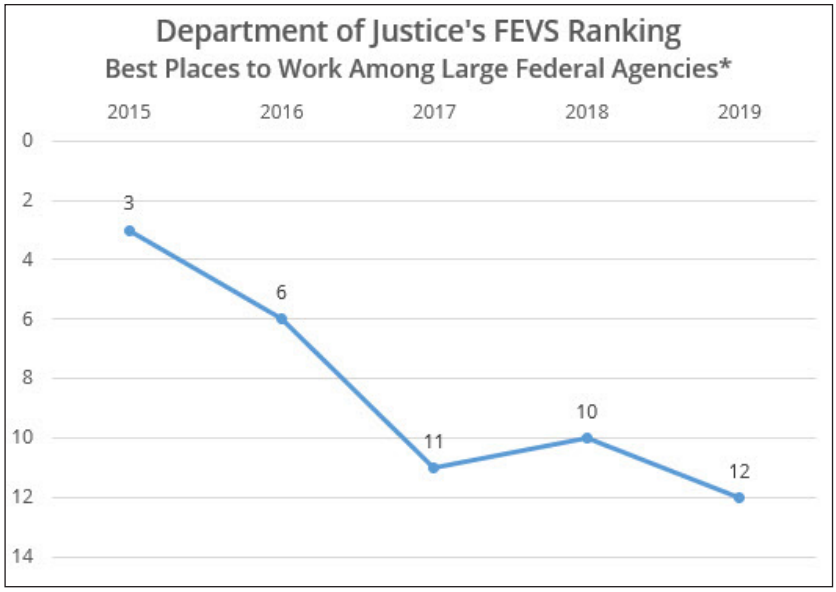
In addition, the OIG has significant concerns regarding components' ability to capture, track, and utilize data to improve operational performance. For example, in a February 2020 review, the OIG found that BOP needs to ensure that institutions track and report all of their prescription drug purchases for inmate health care, not just those from prime vendors. This review highlighted that additional data was necessary and analyzing existing data thoroughly would assist the BOP in its efforts to control costs, seek more favorable drug prices, and reduce waste resulting from unused drugs. The need to collect additional data and analyze existing data was also noted in a June 2019 audit in which the OIG found that Department components were not adequately monitoring and tracking appropriate data on sponsored foreign nationals used in investigations and prosecutions, even though tracking these individuals is critical to protect the public. The OIG's audits and reviews of various components indicate that performance-based management is an issue that the Department should address in order to gain efficiencies in programs and better achieve goals.

"We recommend that the DEA enhance its outcome-oriented performance measurement strategy to clearly define programs goals prior to project implementation, ensure an evidence-based assessment of those goals during and after project completion, and include a focus on program sustainability."

Audit of the DEA's Community-Based Efforts to Combat the Opioid Crisis

The Department's Challenge to Enhance Human Capital

To achieve the goal of "good government" as identified in the DOJ Strategic Plan, one of the Department's strategies is to employ, develop, and foster a collaborative, qualified, high-performing, and diverse workforce. The 2019 Federal Viewpoint Survey (FEVS) results highlight that the Department scored poorly in several categories, causing the Department's ranking among best places to work among the large federal agencies to decline from 2015 to 2019. Some of the FEVS categories include effective leadership, work-life balance, support for diversity, training and development, and performance-based rewards and advancement. A low FEVS ranking reflects and impacts the Department's ability to recruit and retain employees. Although the Department's mission



*The number of large agencies included in this ranking was 19 in 2015, 18 in 2016 and 2017, and 17 in 2018 and 2019.

Source: Best Places to Work

remains a strength, the market for top talent is highly competitive. Thus, in furtherance of its goal of employing a high performing and diverse workforce, the Department and each component should take action to improve in each of the FEVS categories reflected.

Highly Skilled Professionals. The Department faces challenges recruiting and retaining employees to fill certain mission-critical positions. For example, the Attorney General's July 2018 Cyber-Digital Task Force report describes ongoing challenges in recruiting and retaining experienced cyber investigators and attorneys, who are offered higher salaries in the competitive private sector. As noted in previous years' TMPC reports, healthcare and cyber-professionals are highly sought in the private sector and often receive salaries that cannot be matched with the federal pay scale.

For example, as noted in the Prisons section of this report, the BOP had a 16 percent vacancy rate for correctional officers as of June 2020, amounting to 3,350 unfilled correctional officer positions. Furthermore, in a 2016 report, the OIG found that the BOP had only staffed 83 percent of the positions providing medical care to inmates. Such staffing issues have been compounded by the ongoing pandemic. For example, a July 2020 OIG inspection revealed that a shortage of medical staff and correctional staff at FCC Lompoc negatively impacted the facility's ability to screen inmates and staff for COVID-19 and implement strategies to mitigate the impact of the pandemic on inmates and staff.

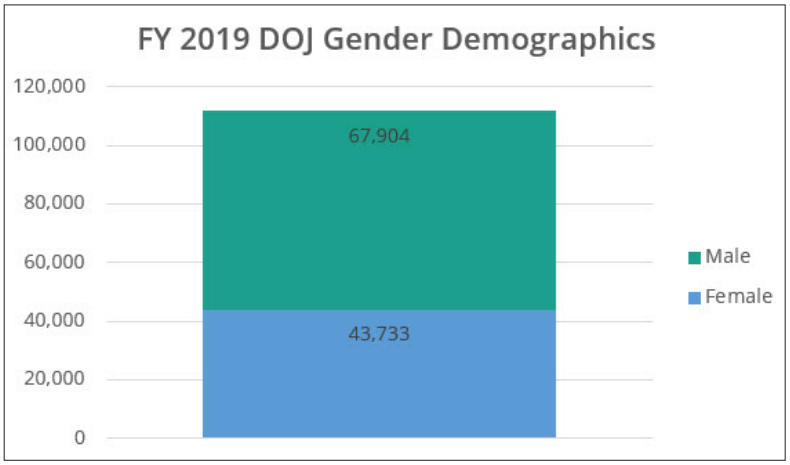
Additionally, in a March 2020 audit, the OIG found that the FBI's Western New York Regional Computer Forensic Laboratory (WNYRCFL), which was created in response to law enforcement's urgent demand for expert digital forensic services, struggled to meet performance goals due to the difficulty in recruiting qualified examiners, which in turn, increases the risk of future forensic examination backlogs. The OIG is conducting an ongoing audit of the FBI's National Security Undercover Operations, which includes an evaluation of the FBI's efforts to recruit and train agents for undercover operations.

Both the President and the Department have recently reinforced the need to promote effective hiring strategies. On June 26, 2020, the President issued Executive Order 13932 which requires agencies to review and revise job classification and qualification standards based on the concern that, "an overreliance on college degrees excludes capable candidates," especially for jobs related to "emerging technologies." This Executive Order further requires agencies to "continually evaluate the effectiveness of different assessment strategies to promote and protect the quality and integrity of their hiring processes." The Department's FY 2021 Performance Plan states, "In an effort to recruit and judiciously hire top talent to carry out the DOJ mission, the Department's Human Resource Administration will work to enhance recruitment and outreach strategies to attract and retain top talent by improving the Departmental backfill rate by 3 percent and reducing the attrition rate by 1 percent." The Department's challenge is to continuously fill vacant and new positions with top-notch employees who can effectively fulfill the DOJ mission.

Work Life Balance. In addition to improving hiring practices, the Department should work within existing laws and regulations to provide competitive compensation packages and work-life opportunities. A 2014 Presidential Memorandum highlighted that to attract and retain a talented and productive workforce, the Federal Government must make progress in enabling employees to balance their responsibilities at work and at home. The Department scored in the lower median of large federal agencies in the work-life balance category for the 2019 FEVS, continuing a downward trend for 3 consecutive years. Recently, OPM established a

number of temporary work-life flexibilities to help employees address the changing demands of home and work resulting from COVID-19. The Department adopted OPM's expanded flexibilities in a memo to the heads of Department components and U.S. attorneys. Some workplace flexibilities adopted include an expanded telework program, evacuation pay, and expanded alternative work schedules. Congress also enacted the Federal Employees Paid Parental Leave Act, effective October 1, 2020, to further help employees juggle the demands of work and family life when a new child is added to the family. On August 10, 2020, OPM issued interim regulations providing additional guidance on the implementation of this new law. Although the sensitive and demanding nature of the Department's work can create a challenge in cultivating work-life balance, the Department should further explore work-life flexibilities.

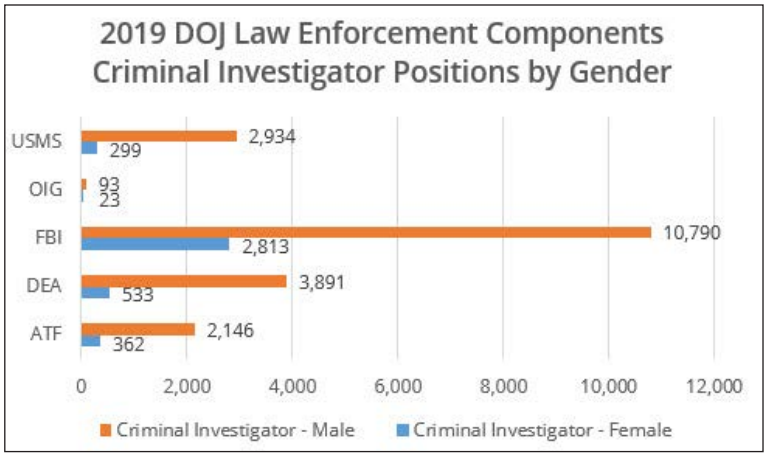
Diversity. Executive Order 13583, "Establishing a Coordinated Government-Wide Initiative to Promote Diversity and Inclusion in the Federal Workforce," provides that "we are at our best when we draw on the talents of all parts of our society, and our greatest accomplishments are achieved when diverse perspectives are brought to bear to overcome our greatest challenges." As a result of Executive Order 13583, OPM established a government-wide strategic plan for agencies to foster diversity in the applicant pool, workforce engagement, and inclusion. However, the Department's 2019 FEVS score for "Support for Diversity" continued a decline that started in 2016. On September 22, 2020, the President issued Executive Order 13950, which stated that "federal agency diversity and inclusion efforts shall, first and foremost, encourage agency employees not to judge each other by their color, race, ethnicity, sex, or any other characteristic protected by Federal law." This order also mandated that agencies review and have OPM approve their Diversity training programs to ensure compliance with specified criteria. As a result, diversity training within the Departments and its components was suspended pending OPM approval.



Source: DOJ Employee Factbook

In June 2018, in a Review of Gender Equity in the Department's Law Enforcement Components, the OIG found that only 16 percent of the Department's Criminal Investigators were women and few held law enforcement executive leadership positions. Moreover, the review found that female criminal investigators frequently reported gender discrimination and both men and women believed that personnel decisions, such as promotions, were based on personal relationships instead of merit. Furthermore, the DOJ Gender Equality Network expressed diversity concerns with respect to the lack of women in executive level management and to worrisome hiring practices that perpetuate gender inequality. Additionally, the DOJ Pride Network indicated that many LGBTQ employees felt unwelcomed at the DOJ.

The OIG is currently conducting a review of gender equity in FBI's training and selection processes at the FBI Academy. In addition, the OIG has received and investigated numerous



Source: DOJ Employee Factbook

allegations over the past several years of inappropriate relationships and favoritism within the Department and its components. These investigations have led to several findings of inappropriate relationships, harassment, and favoritism, which can greatly impact the workforce. As a result of these investigations, we also determined that the components have differing policies governing supervisor-subordinate relationships, which have led to inconsistent disciplinary treatment and, thus, could undermine confidence in the fairness of the Department's disciplinary system. We issued a MAM recommending that the Department determine whether to adopt a consistent policy regarding the handling of supervisor-subordinate relationships across DOJ components.