U.S. Department of Justice
Office of the Inspector General

Top Management and Performance Challenges Facing the Department of Justice–2021

Date: October 15, 2021

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 2021 report on the top management and performance challenges facing the Department of Justice (the 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 Trust in the U.S. Department of Justice
- The Department's Contingency Planning Post-Pandemic
- Maintaining a Safe, Secure, and Humane Prison System
- Countering Domestic and International Terrorism and Safeguarding National Security
- Protecting the Nation and Department against Cyber-Related Threats and Emerging Technologies
- Strengthening Community Engagement, Law Enforcement Coordination, and the Response to Violent Crime
- Managing the Opioids/Fentanyl Crisis
- Managing Human Capital
- Ensuring Financial Accountability of Department Contracts, Grants, and Pandemic-Related Funds

We believe that strengthening public trust in the Department is an urgent challenge that will continue to garner significant public attention, and that will require meaningful action from the Department. This challenge encompasses the important topics of demonstrating independence from political influence, providing leadership to the law enforcement community in protecting First Amendment activity while ensuring public safety, increasing transparency and accountability through implementation of a body worn camera program, and demonstrating the ability to effectively administer justice. Many of these issues are not new challenges, but recent events make the Department's attention to them even more critical.

Managing the prison system, which always presents significant challenges, has been particularly difficult during the Coronavirus Disease 2019 (COVID-19) pandemic. Typical issues, such as staffing shortages and providing inmate healthcare and programming, have been exacerbated by the need to mitigate COVID-19 in Federal Bureau of Prisons facilities. The Department faces other unprecedented and complex challenges related to the pandemic, including adapting its human capital policies and enhancing its planning for future emergencies and catastrophic events.

In addition, enhancing national security remains a key challenge for the Department. While foreign terrorist organizations and espionage are perennial concerns, the rising danger of homegrown violent extremism and intersecting threats of domestic terrorism and hate crimes require the Department to expand the focus of its role in protecting the homeland and our democracy. Other challenges have also become more complex. Cyber-related intrusions are increasingly prevalent and represent a significant threat to the federal government, the American economy, U.S. public discourse, and American elections. Enhancing trust between police and communities, increasing coordination across all levels of law enforcement, combatting violent crime and the opioids crisis, and managing contract and grant awards are ongoing challenges that have been affected by the pandemic, as well as national and world events. The report also highlights the importance of maintaining a workplace that is free of sexual misconduct and harassment, and of leveraging workplace flexibilities and maximizing diversity, equity, and inclusion to recruit and retain a highly skilled and effective workforce.

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

Attachment

Table of Contents

Strengthening Public Trust in the U.S. Department of Justice

A significant challenge facing the U.S. Department of Justice (DOJ or the Department) is how it can strengthen public trust in its ability to impartially and effectively enforce the nation's laws. This critical function is deeply rooted in the Department's history and in its policies and guidelines. Not only does the Department identify ensuring the "fair and impartial administration of justice for all Americans" as part of its fundamental mission, the Justice Manual, a collection of general policies and guidance relevant to the work of federal litigators and legal advisors, mandates that the Department's legal judgments and prosecutorial decisions be "impartial and insulated from political influence." Public discourse questioning the objective application of law is concerning and must be addressed.

Maintaining Independence from Political Influence by Adhering to and Strengthening Policies Designed to Ensure Objectivity and Impartiality

The Department faces a challenge in addressing public perception about its objectivity and insulation from political influence. A 2020 report by the Pew Research Center (Pew) showed that DOJ had one of the lowest ratings among federal agencies. In March 2020, Pew surveyed 1,013 U.S. adults and asked them if their overall opinion of 10 federal agencies was very favorable, mostly favorable, mostly unfavorable, or very unfavorable. Of the 10 agencies included in the survey, DOJ ranked ninth, with only U.S. Immigration and Customs Enforcement polling less favorably. While the overall favorability rating of DOJ has increased since its low point in 2015, the data suggests a concerning trend: the political affiliation of the survey respondents seemed to affect their view of the Department. As Pew noted, unlike many federal agencies, the view of the Department was starkly divided by political affiliation. While prior Pew surveys have shown a disparity between political affiliation and the favorability of the Department, the recent 2020 survey evidenced the widest disparity since 2010. A comparison with prior Pew surveys also shows that the disparity has been increasing since the same survey was conducted in February 2018, when the Department scored similar overall favorability ratings, but this view was shared almost equally by both political affiliations.

Great Hall of U.S. Department of Justice Building (Robert F. Kennedy Building)
Source: U.S. Marshals Service

One important strategy that can build public trust in the Department is to ensure adherence to policies and procedures designed to protect DOJ from accusations of political influence or partial application of the law. As we found in a prior report examining various actions taken during the 2016 election, decisions to deviate from the Federal Bureau of Investigation's (FBI) and the Department's established procedures and norms negatively impacted the perception of the Department as a fair administrator of justice. Similarly in another report concerning then-FBI Director Comey's disclosure of certain investigative information, we observed that it is of the utmost importance to adhere to Department and FBI policies—particularly when confronted by what appear to be

Strengthening Public Trust in the U.S. Department of Justice

extraordinary circumstances or compelling personal convictions. And where the FBI failed to adhere to its own policies, an Office of the Inspector General (OIG) review of certain aspects of the FBI's Crossfire Hurricane investigation noted that such failures have the potential to affect the FBI's reputation as one of the world's premier law enforcement agencies.

Numerous national events in the past year have crystalized the urgency for the Department to address this challenge in a meaningful way. Public reports that political considerations allegedly influenced the Department's decision to obtain communications of members of Congress and the media, accusations that lawful protestors were cleared from Lafayette Square for political purposes, as well as claims that some Department officials may have sought to take action to alter the outcome of the 2020 Presidential Election have all raised questions about the Department's objectivity and impartiality. In June 2021, the OIG announced a review that will examine the Department's compliance with applicable DOJ policies and procedures in using subpoenas and other legal authorities to obtain communication records of members of Congress and affiliated persons, as well as the news media, in the Department's investigations of unauthorized disclosures of information. This review will also encompass whether any such uses, or the investigations, were based upon improper considerations. The OIG also initiated a review of the Department's roles and responsibilities in responding to protest activity and civil unrest on June 1, 2020, at Lafayette Square. The OIG will examine DOJ law enforcement personnel's compliance with applicable identification requirements, rules of engagement, and legal authorities. The review will also consider law enforcement personnel's adherence to DOJ policies regarding the use of less-lethal munitions, chemical agents, and other uses of force. A third review will examine whether any former or current DOJ official engaged in an improper attempt to have the Department seek to alter the outcome of the 2020 Presidential Election. The OIG's work on these and other matters, and any forthcoming guidance and recommendations, should provide the Department assistance with addressing public concerns about the Department's objectivity, impartiality, and independence from political influence.

Improving Public Trust Through Effective Law Enforcement, Adherence to Policies, Strong Interagency Coordination, and Vigorous Oversight

In addition to public perceptions about objectivity and independence from political interference in the Department's decision making, DOJ faces the challenge of protecting the public and enforcing the law at the same time there has been an erosion of public confidence and trust in law enforcement. Over the past several years, numerous high-profile incidents involving serious misconduct by law enforcement, including George Floyd's murder in May 2020, have contributed to this loss of public confidence. One of the most significant challenges facing the Department is strengthening trust between the police and communities. Enhancing trust is critical because a constructive relationship between the police and the communities they serve is essential to effective policing.

National Night Out, in Lincoln Park, Washington, D.C., August 3, 2021
Source: U.S. Marshals Service

Strengthening Public Trust in the U.S. Department of Justice

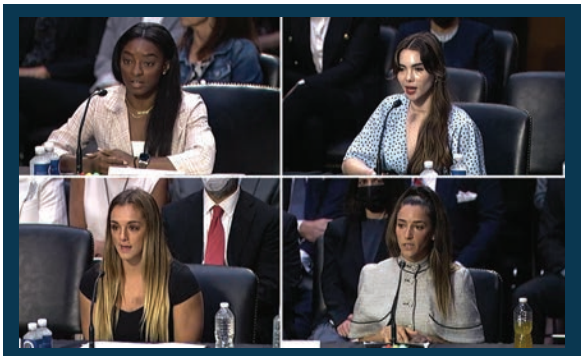
Maintaining Independence from Political Influence by Adhering to and Strengthening Policies Designed to Ensure Objectivity and Impartiality

Improving Public Trust Through Effective Law Enforcement, Adherence to Policies, Strong Interagency Coordination, and Vigorous Oversight

A Commitment to Transparency and Accountability Can Build Public Trust in the Department

The Strengthening Community Engagement, Law Enforcement Coordination, and the Response to Violent Crime section of this report discusses the challenges faced by the Department in greater detail. Law enforcement failures, including those that violate civil rights, affect public safety, and undermine individuals' privacy rights, damage public trust and have lasting effect. Effective law enforcement, strong interagency coordination, careful adherence to policies governing sensitive investigative authorities, and vigorous oversight of law enforcement are important components of the Department's effort to maintain its integrity and the integrity of all law enforcement.

Additionally, as described in the Department's Strategic Plan for Fiscal Years 2018–2022, one of the strategic goals of the Department is to promote public safety. Ensuring that law enforcement handles investigations that affect public safety appropriately and effectively is an important challenge facing the Department. When law enforcement fails to do so, public safety is compromised, which can, in turn, impact the public's trust. For example, the OIG's investigation and review of the FBI's handling of allegations of sexual abuse by former USA Gymnastics physician Lawrence Gerard Nassar details a series of failures in the FBI's investigation that underscores the significance of this challenge. The OIG found that FBI senior officials failed to respond to allegations of sexual abuse with the utmost seriousness and urgency that they deserved and required. Among the failures was the lack of expeditious notice to state and local law enforcement, or other FBI field offices with stronger jurisdictional links to the allegations, in order to mitigate the ongoing danger posed by Nassar. In a statement, the FBI acknowledged its actions and inactions were a "breach of trust." In light of these findings, the FBI advised the OIG that it has reviewed applicable policies, procedures, training, and programs, and is in the process of making changes to strengthen the FBI's handling of future sexual abuse allegations. The OIG's oversight will continue through its review of the FBI's implementation of the OIG's recommendations.



Gymnasts Simone Biles, McKayla Maroney, Maggie Nichols, and Aly Raisman testified before the Senate Judiciary Committee
Source: Screenshot from Senate Judiciary Committee Video on September 15, 2021

As part of its continuing oversight of the effectiveness of DOJ's law enforcement response to public safety threats, the OIG has initiated a review of DOJ's preparation for and response to the events at the U.S. Capitol on January 6, 2021. This review will include an examination of whether there are any weaknesses in Department protocols, policies, or procedures that adversely affected DOJ's ability to effectively prepare for and respond to these events.

Another challenge for the Department is coordinating actions among DOJ components and other federal, state, and local stakeholders to ensure that it appropriately and effectively exercises its law enforcement responsibilities. A recently published OIG report about the Department's implementation of the "zero tolerance policy" highlights how the lack of coordination among different agencies and branches of the government

can have a substantial public impact. In that review, the OIG found that senior DOJ officials failed to coordinate the policy with relevant U.S. Attorney's Offices, the U.S. Marshals Service, the U.S. Department of Health and Human Services, or the federal courts. The review found that the Department's single-minded focus on increasing immigration prosecutions came at the expense of careful and appropriate consideration of the impact that such prosecutions and resulting family separations would have on children and the government's ability to later reunite the children with their parents.

DOJ continues to face the additional challenge of ensuring that, in exercising sensitive law enforcement authorities, its components adhere to policies designed to protect individuals' civil liberties and privacy. Although issues arising from the FBI's use of authorities under the Foreign Intelligence Surveillance Act (FISA) were previously addressed in the 2020 Top Management and Performance Challenges (TMPC) report, and the FBI has made important strides to address the OIG's recommendations since issuance of the Crossfire Hurricane report in December 2019, significant work in this area remains. In September 2021, the OIG released an audit report that confirmed that problems with implementation of the FBI's factual accuracy review procedures ("Woods Procedures") were not isolated to the FISA applications examined in our Crossfire Hurricane review. Our latest report made 10 recommendations to the FBI and the National Security Division to strengthen the Woods Procedures and reduce the risk of erroneous information being included in FISA applications, which can lead to faulty probable cause determinations and the infringement of U.S. persons' civil liberties. At the time the report was published, the FBI and the National Security Division had taken sufficient action to close 5 of the 10 recommendations issued to them collectively. The OIG is also conducting an audit of 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.

A Commitment to Transparency and Accountability Can Build Public Trust in the Department

The Department can also strengthen public trust by enhancing transparency and accountability. Two steps DOJ can take to improve transparency and accountability are requiring the use of body worn cameras by its law enforcement personnel and ensuring that Department employees who engage in misconduct are appropriately disciplined.

Body Worn Cameras and New Department Policies Requiring Their Use

Body worn cameras (BWC) are an important tool that can enhance law enforcement transparency and accountability, and thereby assist in building and maintaining public trust. For years, in an effort to help promote the use of BWC systems by local law enforcement agencies nationwide, DOJ has promoted state, local, and tribal law enforcement use of BWCs. Since 2015, the Department, through the Office of Justice Programs, has provided over $115 million in grant awards to fund BWC programs, including $102.7 million in direct assistance to over 400 state, local, and tribal law enforcement agencies to establish or improve their BWC programs, and $12.5 million in training and technical assistance. During the last year, the importance of BWCs for federal law enforcement has been illustrated by national events including the Department's deployment of law enforcement during civil protests at Lafayette Square and its response to the riot at the U.S. Capitol. In both of these instances, the lack of use of BWC's by federal law enforcement components has impacted the Department's ability to

Strengthening Public Trust in the U.S. Department of Justice

address complaints of misconduct by law enforcement and investigate criminal acts against law enforcement and the public.

In the OIG's June 2021 report examining the Department's policy regarding use of BWCs by its law enforcement personnel, we found that the Department-wide guidance would benefit DOJ components and assist federal prosecution efforts in excessive use-of-force cases. Shortly before the report's release, Deputy Attorney General Lisa Monaco announced a new policy requiring its law enforcement officers to use BWC's when executing search and arrest warrants, which we believe is an important step toward increased transparency and accountability.

Accountability Among DOJ Employees

Holding Department personnel accountable for their misconduct remains an essential element of strengthening the public's trust in DOJ. Accountability is particularly challenging in instances where the Department employee retires or resigns before allegations of misconduct can be fully adjudicated. This challenge was acknowledged by FBI Director Christopher Wray in recent testimony before the Senate Judiciary Committee concerning the FBI's handling of the Nassar investigation. Indeed, a recent OIG review found that, in more than 10 percent of the misconduct cases pending before the FBI's Office of Professional Responsibility in Fiscal Years 2017 and 2018, the FBI employee retired or resigned prior to the disciplinary process being completed. We further found that the FBI's Office of Professional Responsibility closed those cases without regularly documenting substantiation decisions. We concluded that this FBI practice adversely impacted the FBI's ability to hold employees accountable for their misconduct, was unfair to employees wrongly accused, and wasted OIG and FBI resources. Adjudicating all cases to conclusion, as recommended by the OIG, will ensure that employees who choose to leave the FBI while under investigation cannot escape a finding of misconduct that could affect potential future employment and other benefits.

Retirement and resignation pose an additional challenge to the Department's ability to hold its employees accountable. The OIG does not have the authority under the Inspector General Act to compel the testimony of witnesses who are not currently employed by the Department. The lack of testimonial subpoena authority allows former DOJ officials to shield important information from independent oversight and limits the OIG's ability to secure statements from other critical non-DOJ witnesses, both of which detrimentally impact the OIG's ability to hold employees accountable for their misconduct and ensure that Department personnel are using their legal authorities appropriately. Testimonial subpoena authority would foster accountability and strengthen trust in the Department.

The OIG's work to protect whistleblowers from retaliation implicates both of the concerns cited above. Whistleblowers perform an important service for the public and the Department when they report evidence of wrongdoing, and they should never be retaliated against for making such disclosures. The OIG has primary jurisdiction to investigate allegations of reprisal by employees of the FBI and Department contractors and grantees, and we also seek to protect any employee who brings information to the OIG. These efforts are undermined when the subject of a reprisal claim retires or resigns during the course of a whistleblower investigation, undermining the OIG's ability to hold that official accountable, and, without the ability to compel testimony from non-DOJ witnesses, limits our ability to gather all relevant information related to the alleged reprisal. The recommendations and policy reforms cited above would improve our efforts to protect

Strengthening Public Trust in the U.S. Department of Justice

Maintaining Independence from Political Influence by Adhering to and Strengthening Policies Designed to Ensure Objectivity and Impartiality

Improving Public Trust Through Effective Law Enforcement, Adherence to Policies, Strong Interagency Coordination, and Vigorous Oversight

A Commitment to Transparency and Accountability Can Build Public Trust in the Department

conscientious whistleblowers and hold government and contractor officials accountable for retaliating against whistleblowers.

Finally, as noted in the 2020 TMPC report,another means of strengthening confidence in the Department is ensuring that attorney professional misconduct matters are handled no differently than misconduct allegations made against law enforcement agents or other DOJ employees. Currently the Department's Office of Professional Responsibility, a DOJ component that lacks the same statutory independence and protections as the OIG, has exclusive jurisdiction over allegations of misconduct by Department lawyers that relate to an attorney's responsibility to investigate, litigate, or provide legal advice. Independent oversight of Department lawyers is a step towards broader accountability and improved public trust in the Department.

The Department's efficacy as the guardian of the rule of law depends on maintaining the public trust in its integrity, impartiality, and ability to effectively administer justice. Strengthening policies and ensuring adherence to existing policies will assist the Department in maintaining and improving public trust in law enforcement's actions and decision. Robust oversight of the Department's policymaking, including policies designed to improve interagency coordination, can also help the Department meet this challenge. Improving transparency and accountability are two additional tools that the Department can rely on to strengthen the public's trust in its actions as well as the actions of its law enforcement components.

The Department's Contingency Planning Post-Pandemic

Lessons Learned about Pandemic Preparedness and Response

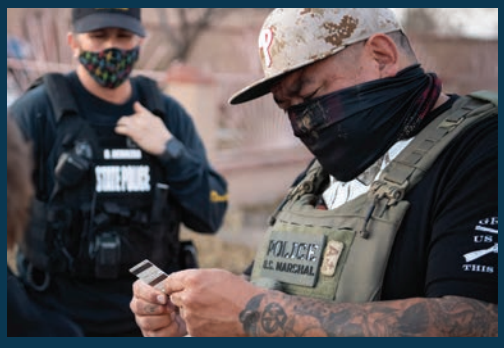
Responding to the rapidly evolving Coronavirus Disease 2019 (COVID-19) pandemic presented immediate and significant challenges for the Department of Justice (DOJ or the Department), some of which remain ongoing. The Department continues to face unprecedented and complex issues in meeting its responsibility to keep its employees, contractors, visitors, and workspaces safe. In addition to protecting its own workforce while continuing to perform its critical mission, most notably, DOJ encountered urgent and critical challenges arising from the pandemic in connection with its responsibility to maintain safe and secure custody of over 156,000 federal inmates and over 64,000 detainees (as of October 7, 2021) in the custody of the Federal Bureau of Prisons (BOP) and the U.S. Marshals Service (USMS). The pandemic also presented issues with the operation of the nation's immigration courts in a manner that minimized health risks to parties and employees, while preserving individual rights. The challenges confronted by the Department in responding to the COVID-19 pandemic can inform and refine its planning and preparedness for future emergencies and catastrophic events. The test for the Department is to apply lessons learned during the pandemic to date in addressing the ongoing issues presented by this public health tragedy, as well as to enhancing its contingency planning for other emergencies and catastrophic events.

Lessons Learned about Pandemic Preparedness and Response

The COVID-19 pandemic has forced the Department to evaluate policies and procedures to maintain the safety of its workforce and the public, and that effort remains ongoing. In March 2020, the Office of the Inspector General (OIG) shifted a significant portion of its oversight efforts toward assessing various DOJ components' responses to the emerging COVID-19 pandemic. Since that time, these efforts have been expanded to include areas such as the impact of COVID-19 on DOJ law enforcement and other Department operations. Through these reviews assessing various components' responses and handling of issues arising from the COVID-19 pandemic, the OIG has offered recommendations to help the Department strengthen its readiness for future pandemics and other catastrophic events.

Impact of COVID-19 on Department Operations

The OIG's oversight work revealed that the effects of the pandemic were felt across the Department, disrupting not only the operations of the BOP, USMS, and Executive Office for Immigration Review (EOIR), but also court proceedings, criminal investigations and prosecutions, and civil and administrative matters. As part of a review of the Department's pandemic readiness, the OIG conducted a survey of DOJ's law enforcement and litigating components to assess the effects of COVID-19 on operations. Survey results from the law enforcement agencies indicate that two-thirds of respondents believe COVID-19 has affected federal law enforcement operations, with the majority of respondents indicating that there had been no formal screening procedure for its agents. As a result, the OIG recommended



Law enforcement officers wear face coverings during Operation Washout in Roswell, New Mexico, in November 2020
Source: U.S. Marshals Service

The Department's Contingency Planning Post-Pandemic

Lessons Learned about Pandemic Preparedness and Response

action items such as implementing COVID-19 screening procedures and testing at worksites. The OIG is currently working on two surveys of DOJ litigating components to better understand the effects of COVID-19 and the anticipated work conditions for the post-pandemic work environment.

Although the unprecedented conditions of the pandemic could not be anticipated, the Department will need to be attuned to the effects of these conditions on its employees and on DOJ operations in its continued response to the pandemic, and its return-to-work planning. The OIG survey results and inspections revealed that DOJ will need to better prepare for possible future emergency and catastrophic events by, for example, addressing existing physical infrastructure and staffing issues, ensuring the availability of information technology (IT) resources, and having robust policies in place should a need arise again to physically distance and pivot to a virtual work environment.

BOP's Preparedness and Response to the Pandemic

The BOP is responsible for providing a safe and secure environment for the federal inmate population, and the safety of its staff. These responsibilities presented significant challenges during the pandemic, first among them being mitigating the spread of COVID-19 in its facilities. As of October 25, 2021, the Department was responsible for housing over 155,000 federal inmates and ensuring the safety of over 37,000 staff. Since the onset of the pandemic through October 24, 2021, according to OIG analysis of BOP data, the BOP has seen nearly 43,000 inmates and over 8,000 staff recover from COVID-19, while 265 inmates and 7 staff have died as a result of COVID-19.

In March and April 2020, the OIG initiated 16 remote inspections of facilities housing BOP inmates, including 11 BOP-managed facilities, 3 contract prisons, and 2 Residential Reentry Centers (RRC). The objective of the inspections was to evaluate the response to the pandemic at each inspected location. Between July 2020 and March 2021, the OIG issued 15 reports[1] providing the results of these inspections. In addition, beginning in October 2020, the OIG began posting to its public website a collection of interactive dashboards with updated data related to COVID-19 in BOP facilities.

FCI Terminal Island Converted UNICOR Facility
Source: BOP, with OIG enhancement

The OIG found common concerns among the facilities at which it conducted remote inspections. One of our repeated findings was the ineffective application of Coronavirus Aid, Relief, and Economic Security (CARES) Act and Attorney General authorities allowing expanded use of home confinement to mitigate the effects of COVID-19 in BOP facilities. In particular, the OIG determined that in some of the institutions inspected, the BOP failed to broadly consider home confinement for inmates with short remaining sentences, instead focusing its use of this authority

[1] One of the reports issued in November 2020 encompassed two remote inspections at FCCs Oakdale and Pollock.

The Department's Contingency Planning Post-Pandemic

Lessons Learned about Pandemic Preparedness and Response

primarily on inmates with enhanced vulnerability to the disease, which was one of the bases permitted by the Attorney General's directive. This reticence to using its home confinement authority is consistent with the results of prior OIG reviews on the BOP's use of its compassionate release and international treaty transfer authorities.[2]

In addition, the OIG found that infrastructure and supply issues impeded the BOP's ability to effectively respond to the pandemic. For example, BOP locations with open style floor plans (such as seen at Metropolitan Correctional Center Chicago, Federal Correctional Complex (FCC) Butner, and at FCC Oakdale), were faced with significant challenges mitigating the transmission of COVID-19. Other institutions had to contend with space limitations that affected the ability to allow for proper social distancing (as seen at Federal Correctional Institution (FCI) Terminal Island and Federal Medical Center (FMC) Fort Worth), which also had an impact on mitigation efforts. Multiple BOP and contract facilities dealt with issues around the availability or appropriate use of Personal Protective Equipment by staff or inmates (as seen at FCC Coleman, Metropolitan Detention Center (MDC) Brooklyn, Brooklyn House RRC, and Toler House RRC).

As discussed in greater detail in the Maintaining a Safe, Secure, and Humane Prison System section of this report, staffing shortages, including difficulty recruiting and retaining medical staff, have been a persistent challenge for the BOP. The OIG's remote inspections found that the existing staffing shortages significantly undermined the BOP's ability to respond to the pandemic and provide appropriate healthcare to inmates. For example, the OIG found that a rapid COVID-19 outbreak in April and May of 2020 at FMC Fort Worth resulted in a large number of inmates being transferred to local hospitals for treatment, which required correctional officers to be reassigned to local hospitals, thus creating staffing challenges that affected the response to the conditions. Additionally, the OIG's inspection at FCC Lompoc revealed that the preexisting shortage of medical staff was among the biggest challenges in mitigating COVID-19 transmission because of the burdens of screening inmates and staff members for COVID-19 symptoms while still providing routine medical care to the institution's approximately 2,700 inmates.

The OIG also found that BOP facilities did not consistently adhere to COVID-19 protocols to ensure the safety of staff and inmates. For example, at FCI Milan staff escorted at least one, and possibly more, inmates with COVID-19 symptoms to a local hospital without wearing appropriate Personal Protective Equipment, which potentially contributed to an increased risk of those staff contracting COVID-19 and the spread of COVID-19 within FCI Milan. In addition, we found that the BOP needs to provide clear and timely guidance to contract prisons and coordinate with various stakeholders, such as the federal courts, U.S. Attorney's Offices, public defender offices, and others to ensure a consistent and safe approach in emergency situations. The BOP can draw upon these OIG findings relating to infrastructure, staffing, supplies, health and safety protocols, and coordination with other criminal justice entities in its continuing efforts to mitigate the effects of COVID-19 at its facilities, and to prepare for other health and related emergencies.

The OIG is conducting further oversight of the BOP's response to the pandemic and expects to issue additional products to assist the BOP with improving its planning and preparedness for emergency conditions. First, the OIG is working on a capstone report that will draw conclusions and

[2] Review of the Imp act of an Aging Inmate Population on the Federal Bureau of Prisons, Evaluation and Inspections Division 15-06 (Revised February 2016); The Federal Bureau of Prisons' Compassionate Release Program, Evaluation and Inspections Division I-2013-006 (April 2013).

make recommendations based on the OIG's findings from across the 15 published remote inspection reports. Second, while the OIG has released the results of a follow-up survey it conducted in 2021 of BOP institution staff, the OIG is completing, and will be publishing, a survey of BOP inmates seeking their perspectives about the BOP's response to the pandemic. Third, the OIG is undertaking a review examining the BOP's use of home confinement as a tool to mitigate the effect of the COVID-19 pandemic on the federal prison population. The review will assess the BOP's process for implementing the use of home confinement as authorized under the CARES Act, the process for its consideration of the eligibility criteria outlined in the Attorney General's March 26, 2020 and April 3, 2020 memoranda, 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. These products will provide the BOP with more information as it works to respond effectively to the ongoing COVID-19 pandemic, as well as in preparing for future catastrophic events that test the BOP's ability to fulfill its mission of providing a safe and secure environment for employees and inmates.

USMS's Response to the COVID-19 Pandemic

The USMS houses detainees in both state and local facilities via Intergovernmental Agreements (IGA) with state and local government detention facilities and in contract facilities across the United States. Facilities that house USMS detainees via IGAs are managed by the local and state authorities or, in some situations, a third-party contractor. Contract facilities are managed directly by the USMS's Prisoner Operations Division. Prior to the pandemic, IGA facilities were traditionally more challenging for the USMS to manage than contract facilities managed directly by the USMS's Prisoner Operations Division, due to the overall lack of influence and control of the IGA facilities.

The OIG's review of the USMS's response to the pandemic from April 2020 through August 2020 revealed that managing IGA operated facilities continues to be a challenge for the USMS. The USMS, therefore, may need to assess how it negotiates IGAs, not only to address cost issues that the OIG identified in prior reports issued in 2011 and 2007, but also to ensure the health and safety of USMS detainees during emergency situations such as the COVID-19 pandemic. In the 2020 review of the USMS's response to the pandemic, the OIG found that facilities managed via IGAs were weaker in the areas of pandemic preparedness, response, and prevention in comparison to the contract facilities. USMS officials told the OIG that it believed this difference was in large part due to the USMS's lesser influence on policies and practices at IGA facilities. The OIG also found that data such as prisoners quarantined due to suspected contact or exposure, staff exposure, and the availability of COVID-19 testing and N95 protective masks were being tracked daily at USMS contract facilities, while they were not tracked at the IGA facilities. As a result of the review, the OIG made six recommendations to the USMS to address issues occurring with its IGA facilities, including requiring the USMS to update its oversight plan for IGA facilities to incorporate the latest Centers for Disease Control and Prevention guidance and conduct in-person reviews of these facilities to ensure such guidance has been implemented. The USMS has implemented new policies and procedures to address the recommendations, which were all closed as of September 2021.

EOIR's Response to the COVID-19 Pandemic

EOIR conducts immigration court proceedings, appellate reviews, and administrative hearings to adjudicate immigration cases in compliance with the federal immigration laws. The OIG's oversight work underscored the

The Department's Contingency Planning Post-Pandemic

Lessons Learned about Pandemic Preparedness and Response

need for EOIR to prepare for future emergency and catastrophic events by modernizing its IT infrastructure, including its filing system and physical IT assets, such as laptop computers, and by improving communication with staff and the public. EOIR's antiquated, paper-based filing system lagged significantly behind other federal and state court systems, and left EOIR particularly vulnerable during the pandemic. Relatedly, the review found that EOIR was insufficiently equipped to enable its employees to conduct functions remotely by teleworking. EOIR did not initially have laptop computers to issue to a significant portion of its staff, and it struggled to adapt its IT infrastructure to accommodate remote work and hearing participation. While EOIR suspended certain dockets due to pandemic conditions, it continued to hear detained docket cases citing due process issues under the Fifth Amendment. Although EOIR judges had some discretion in deciding whether hearings on the detained dockets were postponed, the OIG found in our April 2021 report that filing deadlines remained in place for many immigration cases which, combined with EOIR's continued acceptance of paper filings, increased the risk of COVID-19 exposure, particularly for staff required to process hard copy documents in person. The OIG made nine recommendations to EOIR to modernize its case processing systems, expand the availability of electronic filing, and improve its capability to enable staff to accomplish appropriate tasks via telework. All nine of these recommendations remain open. Addressing these recommendations would better prepare EOIR to cope with emergencies such as the pandemic.

Maintaining a Safe, Secure, and Humane Prison System

The Federal Bureau of Prisons' (BOP) mission is to maintain a safe, secure, and humane prison system. The Coronavirus Disease 2019 (COVID-19) pandemic abruptly presented complexities to the BOP's ability to fulfill its mission, and the ongoing pandemic continues to challenge the BOP. Issues raised by the pandemic exacerbated, or diverted attention from, other longstanding challenges confronting the BOP, such as staffing shortages, contraband, inmate medical care costs, and infrastructure maintenance. We address the pandemic-related challenges facing the Department of Justice (DOJ or the Department) generally, and the BOP specifically, in The Department's Contingency Planning Post-Pandemic section of this report. Accordingly, we focus here on other critical challenges with which the BOP must contend.

Institutional Infrastructure, Physical Safety, and Security

The BOP's mission includes providing safe, humane, cost-efficient, and appropriately secure housing for inmates in its custody. This mission comes with several challenges, including managing the aging infrastructure of 122 institutions as well as implementing new technologies to detect and prevent security risks from entering the institutions. The Office of the Inspector General (OIG) continues to identify work deficiencies in the institutional infrastructure, physical safety, and security of BOP facilities. In a 2019 OIG inspection, we found that Metropolitan Detention Center (MDC) Brooklyn had long-standing unaddressed temperature regulation issues, causing temperatures to fluctuate above and below the BOP's target temperature throughout the facility. Although the BOP has taken some steps to address the infrastructure-related issues at MDC Brooklyn and system-wide that were identified in the report, seven of the nine recommendations remain open. The OIG recently initiated an audit to evaluate the acquisition and construction of new institutions, as well as expansion and maintenance of existing BOP institutions, including how BOP identifies and implements modernization and repair projects. Upon completion of this audit, the OIG expects to provide recommendations to BOP relating to issues presented by its aging facilities and infrastructure.

Another key component of the BOP's mission is to ensure the safety and security of inmates, staff, and the public in the confinement of convicted offenders. The OIG previously highlighted weaknesses in both the BOP's security camera system and its staff screening policy in a 2016 review of the BOP's contraband interdiction efforts. That review found that camera system deficiencies such as known blind spots affect the OIG's ability to secure prosecutions of staff and inmates in BOP contraband introduction cases and adversely impact the accessibility of evidence to support administrative or disciplinary action against staff and inmates. The review also found that the BOP lacked effective deterrence against staff introducing contraband. The 2016 report made 11 recommendations to strengthen the BOP's contraband detection and interdiction efforts, including one recommendation, which remains open, for the BOP to evaluate its existing security camera system to identify needed upgrades, and four recommendations, which also remain open, to strengthen its staff search policy. In June 2021, the OIG issued a Management Advisory Memorandum to the BOP identifying multiple security concerns at BOP camp facilities, including nonfunctional alarms and a lack of video surveillance on exterior doors. Although the BOP has made some progress implementing camera upgrades, because of the critical nature of this ongoing concern, in October 2021, the OIG issued a Management Advisory Memorandum to BOP recommending that it identify enhancements needed to address camera functionality and coverage deficiencies, provide cost projections to

Maintaining a Safe, Secure, and Humane Prison System

fund the upgrades, and include an estimated timeline for completion of the work.

Perimeter security fence at BOP facility
Source: DOJ OIG

Regarding BOP's staff screening deficiencies, an August 2021 Management Advisory Memorandum to the BOP identified urgent security concerns related to staff bypassing security screening upon entering a BOP facility during the night shift. Although this action by staff violated BOP staff screening procedures, it was known to management at the affected facility and tolerated due to staffing shortages. In its memorandum to BOP, the OIG reiterated its concern that BOP's failure to enforce strict staff screening procedures increases the risk that staff will jeopardize the safety and security of the institution, inmates, and other staff by introducing contraband into BOP facilities.

Other OIG work has found additional security-related issues. For example, the BOP continues to be vulnerable to the introduction of contraband via unmanned aircraft systems or drones, as identified in a September 2020 OIG audit. Indeed, in April 2021, as a result of an OIG investigation, a former BOP inmate pleaded guilty to participating in a conspiracy to use drones to smuggle contraband into BOP's Fort Dix prison. Recommendations from our September 2020 audit have not been closed. Additionally, in an audit of the BOP's perimeter security strategy and efforts related to the award of a security-related contract, the OIG identified a need for the BOP to improve its guidelines related to perimeter security and ensure that deficiencies identified and addressed at one facility did not also exist at other similarly situated facilities.

Inmate Healthcare and Welfare

The BOP has long faced challenges with issues surrounding provision of healthcare to inmates in its custody. The most recent manifestation of this issue arose during the pandemic and starkly demonstrated the challenges that the BOP and the Department face. In the OIG's remote inspections of 16 BOP-managed, contract, and Residential Reentry Center facilities, the OIG reported that medical and correctional staffing shortages undermined the BOP's response to the pandemic and impaired its ability to provide adequate medical care to inmates. For example, the remote inspection of MDC Brooklyn found the facility struggled to meet the medical needs of inmates who did not have COVID-19 due to the medical staffing shortage. The OIG made similar findings during inspections at Federal Medical Center Fort Worth, Federal Correctional Complex (FCC) Oakdale, and Federal Correctional Institution (FCI) Milan.

As described in a 2016 OIG review of BOP medical staffing challenges, we found that recruitment and retention of medical professionals is a serious challenge for the BOP in large part because it competes with private employers that offer higher pay and benefits, and because the BOP does not identify or address its recruiting challenges in a strategic manner or

Maintaining a Safe, Secure, and Humane Prison System

Institutional Infrastructure, Physical Safety, and Security

Inmate Healthcare and Welfare

Staffing Shortages

Programs to Reduce Recidivism

take full advantage of staffing flexibilities such as those available through the U.S. Public Health Service. To help the BOP address this challenge, the OIG recommended that the BOP develop strategies to assess and prioritize medical vacancies based on their impact on BOP operations and better utilize U.S. Public Health Service officers to address medical vacancies of the greatest consequence, including the use of incentives, assignment flexibilities, and temporary duty. Although the OIG has closed these recommendations, we continue to find that the BOP faces healthcare provider shortage challenges. For example, the remote inspection of MDC Brooklyn found that a shortage of medical staff hindered the screening of inmates and staff, and MDC Brooklyn struggled to meet the medical needs of non-COVID-19 inmates. Similarly, another OIG remote inspection revealed that at the onset of the COVID-19 pandemic, FCC Coleman operated with only 80 percent of its authorized medical staff, and positive cases exacerbated these staffing shortages.

In addition to challenges in staffing healthcare provider positions within the BOP, costs associated with outside medical providers and pharmaceuticals have been significant and increasing. Healthcare provider staffing shortages factor in the BOP's reliance on outside medical providers. The OIG is conducting an audit of the BOP's comprehensive medical services contracts with the University of Massachusetts Medical School (UMass), which provides offsite and onsite medical care to inmates at three BOP-managed facilities, to assess, among other things, UMass' performance in financial management, monitoring, reporting, and progress toward meeting the contract goals and objectives.

Pharmacy at BOP facility
Source: BOP

Along with an increased need to use outside medical providers, rising pharmaceutical costs have been a burden on the BOP. The BOP attributes its increasing pharmaceutical costs to the increase in overall pharmaceutical industry prices and the aging inmate population. The best price for most drug purchases among federal agencies is the Big 4 price. Big 4 is a discounted government price that is currently accessible to only four government agencies by federal law. In the OIG's review of the BOP's pharmaceutical drug costs and procurement during Fiscal Year (FY) 2012 through FY 2018, the OIG found that, unfortunately, the BOP is not one of these agencies and is paying more for the drugs. The review found that the BOP had made efforts to obtain Big 4 pricing, but the Department was not actively pursuing Big 4 pricing on behalf of the BOP or its other components at the time the report was issued. Both the Department and the BOP must coordinate efforts in order for Congress to pass a statutory amendment to obtain Big 4 pricing. Our review concluded that the BOP's ability to control drug spending is impeded by its inability to obtain drugs at some of the lowest government pricing, by its drug procurement practices and lack of oversight of those practices, and by its insufficient collection and analysis of pharmacy data.

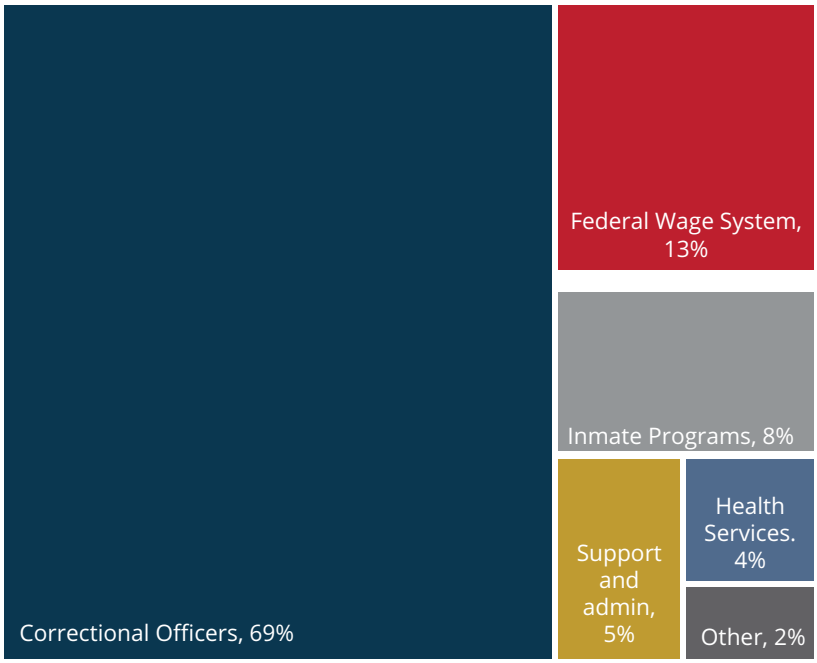
Maintaining a Safe, Secure, and Humane Prison System

Staffing Shortages

Staffing and retention have been a persistent challenge for the BOP. Although the inmate population declined significantly by the end of FY 2020, BOP facilities still struggle with appropriate staffing levels. In a recent U.S. Government Accountability Office (GAO) report, the BOP stated that staffing challenges derive from the geographic locations of BOP institutions, hiring process delays, hiring freezes, and position eliminations. However, the GAO report found that the BOP did not analyze data of staff feedback including exit survey data, annual prison climate survey data, and Federal Employment Viewpoint Survey data to determine if there were additional factors to consider. The GAO concluded that the BOP needed to analyze the feedback as it may reflect additional or different causes and impacts of staffing challenges in the BOP.

Figure 1

Overtime Costs by Occupational Areas



Source: OIG analysis of the National Finance Center's payroll data

A recent OIG Management Advisory Memorandum regarding the BOP's overtime costs noted that inadequate staffing of correctional officer positions was an acute concern for the BOP. In particular, the OIG's analysis of the BOP's FY 2019 overtime costs showed that BOP staff worked over 6.5 million overtime hours, the equivalent of over 3,107 full-time positions. Overtime costs of correctional officers totaled almost 70 percent of the overall overtime costs incurred by the BOP, followed by overtime of BOP employees in positions related to maintaining its facilities, such as equipment maintenance and operations, electrical, and plumbing, as well as food preparation. As the OIG's memorandum makes clear, the BOP needs to develop a comprehensive strategy to address its staffing challenges.

These staffing shortages had a significantly greater impact on the BOP during the early months of the COVID-19 pandemic. For example, the OIG's inspection at FCC Lompoc revealed that the shortage of staff negatively affected the institution's ability to conduct screenings of inmates and staff members for COVID-19 symptoms while also providing routine medical

Maintaining a Safe, Secure, and Humane Prison System

care to the institution's approximately 2,700 inmates. The BOP undertook a temporary solution by deploying temporary duty travel staff from other BOP facilities to FCC Lompoc. A remote inspection report of FCC Oakdale found numerous staff absences during the COVID-19 outbreak, which ultimately forced some institution staff to work more than 40-hour straight shifts. Similarly, the remote inspection of FCI Milan found that 75 percent of its medical staff had contracted COVID-19 by early May 2021, and that COVID-19 staffing shortages among nonmedical staff hampered FCI Milan's efforts to restrict staff movement within the institution to prevent the spread of the virus.

Programs to Reduce Recidivism

Inmate programming is a necessary part of rehabilitation and preparation for reentry into society. That is particularly true for federal inmates because approximately 97 percent of them will reenter society at the end of their sentence. Consistent with that need, the BOP utilizes programs for education, reentry preparation, and religious needs, among others. However, the OIG's 2016 review of the BOP's Release Preparation Program (RPP) identified weaknesses in the BOP's RPPs, including the BOP's lack of a nationwide curriculum to ensure that RPPs across its institutions meet inmate needs, failure to coordinate with other federal agencies to provide access to services that incarcerated inmates need upon release, and inability to determine the RPP's effect on recidivism. Because of inconsistencies in the content and quality of RPP courses, we found that the BOP cannot ensure that all inmates receive the information they need to successfully transition back into the community. The OIG made two policy-related recommendations, both of which remain open. Further, BOP institutions continue to suffer from a lack of programming staff to sufficiently meet the inmates' needs. For example, a July 2021 OIG audit of the BOP's management of its Chaplaincy Services Program found that the BOP lacked service providers to adequately provide services for the diverse faiths found in the inmate population. We reported that 30 percent of its 122 institutions lacked appropriate chaplaincy services staffing under BOP guidelines, and that a lack of faith diversity among the BOP's chaplaincy staff left some inmate faith groups significantly underrepresented. Moreover, while it is critical for the BOP to understand whether its programs are effective in reducing the rate of recidivism so it can modify them as necessary and expand those that are most effective, the BOP has failed to publish a more recent recidivism study since its review of the residential drug treatment programs available to federal inmates in 2001.

The First Step Act of 2018 mandates that the BOP expand programming opportunities and partner with representatives from the community to ensure inmates can develop skills necessary upon release from the BOP. Thus, a significant challenge for the BOP and the Department is ensuring that it has sufficient programming to support inmate needs and meet the requirements of the First Step Act, while also ensuring that its programming is effective in helping inmates transition back into the community and in reducing recidivism.

Countering Domestic and International Terrorism and Safeguarding National Security

Persistent and increasingly sophisticated national security threats arising from malicious domestic and foreign actors can disrupt, degrade, or destroy American economic, socio-cultural, and political interests. Strengthening its ability to design and implement solutions in response to the vast array of national security threats that the country faces today remains a critical challenge for the Department of Justice (DOJ or the Department).

The Department's Preparedness and Response to Domestic Threats

According to the U.S. Department of Homeland Security, the primary terrorist threat inside the United States will stem from lone offenders and small cells of individuals, including Domestic Violent Extremists (DVE) and Homegrown Violent Extremists (HVE). The Federal Bureau of Investigation (FBI) considers DVEs and HVEs two distinct threats. The FBI Director explained in recent testimony that "individuals who commit violent criminal acts in furtherance of social or political goals stemming from domestic influences—some of which include racial or ethnic bias, or anti-government or anti-authority sentiments—are described as DVEs, whereas HVEs are individuals who are inspired primarily by global jihad, but not receiving individualized direction from Foreign Terrorist Organizations." According to the U.S. intelligence community, recent sociopolitical developments will almost certainly spur some DVEs to try to engage in acts of violence in 2021 and beyond. In recognition of the challenge it faces in this area, in June 2020, the Department established a Task Force to Combat Violent Anti-Government Extremism with the goal to understand both HVEs and DVEs "well enough that [the Department] can stop such violence before it occurs and ultimately eliminate it as a threat to public safety and the rule of law." Relatedly, the Department has recognized the intersecting threats of domestic terrorism and hate crimes. After receiving the recommendations from an internal departmental review and the enactment of the COVID-19 Hate Crimes Act and Jabara-Heyer NO HATE Act, Attorney General Merrick Garland issued a memorandum outlining the steps to enhance the effectiveness of DOJ's hate crimes enforcement.

The challenges facing the Department and FBI in this area were exemplified in a March 2020 OIG audit of the FBI's efforts to identify HVEs through counterterrorism assessments, which found that the FBI had not taken a comprehensive approach to resolving deficiencies in its counterterrorism assessment process. Following attacks conducted by individuals who had previously been assessed or investigated by the FBI, the FBI conducted reviews to evaluate its process for assessing potential HVEs, yet the Office of the Inspector General (OIG) found that the FBI had not fully implemented the recommendations that emerged from these prior reviews. Subsequently, the FBI conducted another review to evaluate the investigative thoroughness of closed counterterrorism assessments. While the FBI determined that 6 percent of the closed assessments did not adequately assess the potential threat, the OIG found that nearly 40 percent of those assessments went unaddressed for 18 months after the deficiencies were known to the FBI. The OIG also identified inconsistencies in the FBI's reevaluation of closed counterterrorism assessments, as well as emerging challenges that the FBI must address when assessing potential HVEs. The audit resulted in seven OIG recommendations that aim to assist the FBI in its efforts to identify HVEs through counterterrorism assessments. As of September 2021, all seven recommendations remain open.

Additionally, in September 2021, the OIG initiated an audit of the Department's strategy to address the DVE threat. The preliminary objectives of the audit are to: (1) evaluate the Department's efforts to develop a

Countering Domestic and International Terrorism and Safeguarding National Security

comprehensive strategy to address the DVE threat in the United States, and (2) determine if the Department is effectively coordinating among Department stakeholders on the implementation of its strategy. This audit will focus on Department-level efforts to coordinate an effective approach to identify, investigate, and prosecute DVE threats and promote information-sharing among Department components, as well as with the Department's federal, state, and local partners.

One of the most difficult aspects of combating acts of violence in furtherance of political and social goals is the fact that support for such acts can be closely connected to protected First Amendment speech or activity. Striking the balance between vigorously protecting the security of the nation without impinging upon freedom of expression and other civil liberties is particularly difficult in the context of these domestic threats. In June 2021, Attorney General Garland affirmed that the Department's focus in countering DVE threats is to prevent, disrupt, and deter unlawful acts of violence, regardless of motive, while also recognizing that safeguarding our country's civil rights and liberties is itself a vital national security imperative.

As the National Strategy for Countering Domestic Terrorism makes clear, "[i]n a democracy, there is no justification for resorting to violence to resolve political differences." The OIG's oversight of DOJ's efforts to confront the threat of violent acts in furtherance of political and social goals is ongoing. After the events at the U.S. Capitol on January 6, 2021, the OIG initiated a review that will examine information concerning the January 6 events that was available to DOJ in advance of January 6; the extent to which such information was shared by DOJ with the U.S. Capitol Police and other federal, state, and local agencies; and the role of DOJ personnel in responding to this event. The OIG's review will also assess whether there are any weaknesses in DOJ protocols, policies, or procedures that adversely affected the ability of the Department to effectively prepare for and respond to the events at the U.S. Capitol

Attorney General Garland is briefed by FBI Director Christopher Wray on the events of January 6
Source: DOJ

The OIG also initiated a review to examine DOJ's roles and responsibilities in responding to protest activity and civil unrest at Lafayette Square on June 1, 2020. This review will examine the training and instruction that was provided to 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. The OIG expects that its reporting on these matters will assist the Department with the delicate balancing of protecting the nation's security without sacrificing individuals' civil liberties.

Countering Domestic and International Terrorism and Safeguarding National Security

Counterintelligence and Espionage

The Department's strategic plan identifies hostile intelligence activities and espionage as one of the gravest threats to national security. In addition to foreign governments, hostile foreign actors include non-traditional collectors, foreign corporations, and transnational organized crime groups targeting non-government information. While the threats posed in this area are substantial, the challenge facing the Department and the FBI is that it also must be vigilant in ensuring that it follows policies and processes to ensure investigations are factually predicated and not based on ethnic profiling or other improper considerations. This challenge is exemplified in the OIG's 2019 review of certain aspects of the FBI's Crossfire Hurricane investigation, which demonstrated the importance of safeguarding our country's civil rights and liberties while countering the threats posed by hostile intelligence activities and espionage. Since the release of this report, the FBI has agreed with the report's findings and has already demonstrated its commitment to remedial action by implementing several new initiatives, including evaluating its Foreign Intelligence Surveillance Act (FISA) application and renewal processes and requiring training for employees who handle FISA matters. The OIG will continue to monitor these and other measures taken by DOJ and the FBI to ensure that each of the nine recommendations the OIG made in its review is fully implemented.

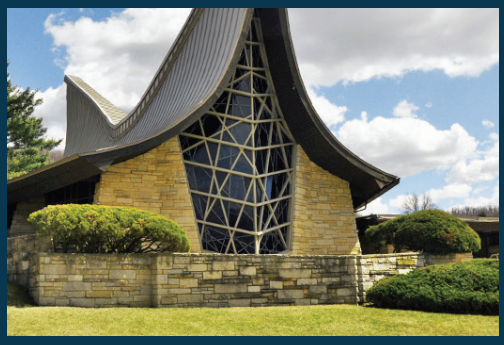
Disrupting and Defeating Foreign Terrorist Operations

Foreign terrorist organizations (FTO) continue to threaten the national security interests of the United States. According to the U.S. Department of Homeland Security, FTOs such as Al-Qaeda and the Islamic State of Iraq and ash-Sham (ISIS) will maintain a high interest in carrying out attacks within the United States. In disrupting and defeating FTOs, DOJ is likely to face many challenges ahead. For example, FTOs continue to probe for vulnerabilities in U.S. immigration and border security programs. FTOs are also increasingly using social media and other online platforms to motivate individuals residing within the United States to carry out acts of terrorism. Further, FTOs are likely to explore the use of unmanned aircraft systems or drones to threaten critical infrastructure or major population centers across the United States. Because of the pervasive threat presented by FTOs, the Department will need to be vigilant and strengthen its response to the national security threats FTOs present.

Throughout Fiscal Year (FY) 2020, the OIG completed several projects that identified several of the high-priority areas of improvement, and challenges, in the DOJ's overall counterterrorism posture for FTOs. For example, in two reports the OIG found that the BOP could take additional steps to mitigate the threat posed by inmates with known connections to terrorism. In March 2020, the OIG completed an audit of the BOP's monitoring of inmate communications to prevent radicalization, which found significant weaknesses in the designation and monitoring of inmates with a known nexus to domestic or international terrorist organizations. The OIG provided the BOP with 17 recommendations, including eliminating the automatic delivery of email to high-risk inmates, determining and maintaining an accurate count of international and domestic terrorists incarcerated at, or in transit to BOP facilities, and improving audio equipment in BOP visiting rooms utilized by terrorist inmates subject to Special Administrative Measure directives. As of September 2021, 13 of the 17 recommendations from this audit remain open.

Further, in July 2021, the OIG completed a report on the BOP Management and Oversight of its Chaplaincy Services Program, which found significant

Countering Domestic and International Terrorism and Safeguarding National Security



BOP chapel facility
Source: BOP

deficiencies in the BOP's ability to prevent inmate access to prohibited content that advocated violence and religious extremism. The OIG also found that the BOP's internal policies do not restrict certain inmates from leading religious services and appear to be inconsistent regarding the level of required monitoring. For example, the OIG found that some institutions permitted inmates with a known nexus to international or domestic terrorism to lead religious services thereby creating a risk that, without clear policy and consistent monitoring efforts, these high-risk inmates could use their religious leadership roles to engage in prohibited activities or as a method to obtain power and influence among the inmate population. The OIG made five recommendations to the BOP to improve the delivery of religious services to the inmate population and to help diversify and alleviate shortages in its chaplain staff.

The OIG has previously found areas for improvement in the FBI's response to terrorist threats. In FY 2019, the OIG completed an audit of the FBI's Management of Maritime Terrorism Threats, and found significant weaknesses that may create an environment in which the FBI could underestimate the risks, threats, and vulnerabilities to the Maritime environment, and miss opportunities to gather intelligence and take actions that could help keep the nation's ports and Maritime assets safe. The OIG made nine recommendations designed to strengthen the FBI's Maritime counterterrorism activities, all of which have been closed.

Combatting Insider Threat and Unauthorized Disclosures

DOJ also faces the challenge of continuing to position itself to detect, deter, and mitigate insider threat risks, which continue to present significant harm to the security of the United States. In its strategic plan, the Department acknowledges insider threats can take on many forms including media leaks, espionage, the unauthorized disclosure of classified information, the theft of intellectual property, violations of export controls or sanctions, or the loss or degradation of Department resources or capabilities. While insider threats and unauthorized disclosures present a serious challenge, the Department must also remain committed to upholding whistleblower rights and protections that allow for DOJ employees or DOJ-affiliated individuals to report wrongdoing in accordance with the laws and rules that govern the release of both unclassified and classified information.

To assist the Department in strengthening its ability to counter insider threats and unauthorized disclosures, the OIG examined the FBI's Insider Threat Program in order to assess insider threat internal controls in 2017. The OIG determined that the FBI needed to improve performance metrics, ensure that insider threats are handled and monitored in a systematic way, pursue technological solutions for stand-alone systems, conduct a comprehensive inventory of classified information technology assets, and monitor user activity over all classified systems and networks. In August 2020, the OIG sent the FBI a memorandum pausing follow-up on these recommendations due to the Coronavirus Disease 2019 pandemic. At that time, all of the recommendations remained open.

Countering Domestic and International Terrorism and Safeguarding National Security

Further, the Department must maintain proper oversight of actions by federal employees or DOJ-affiliated individuals entrusted with national defense information, including contracting staff. The OIG issued a Management Advisory Memorandum in February 2021 after becoming aware that Drug Enforcement Administration (DEA) contractors were not obligated to annually renew their On-Site Contractor Responsibilities document, which prohibits contract employees from engaging in personal and business associations with persons known to be convicted felons or associated with criminal activity. The OIG found this information concerning, as contracting staff are capable of holding sensitive, classified information. The DEA took corrective action and the two recommendations directed towards the DEA were closed in September 2021. The loss, theft, or unauthorized disclosure of classified information by Department employees or contractors can pose a grave threat to the national security of the United States.

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

Cyber breaches and attacks represent a growing threat to individual privacy, economic interests, and national security and is one of the most significant challenges facing the Department of Justice (DOJ or the Department). As outlined in Executive Order (EO) 14028, Improving the Nation's Cybersecurity, the "United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy." As a member of the law enforcement and intelligence community, and as the holder of sensitive and classified information, the Department has a significant responsibility to combat threats such as cyber supply chain attacks and ransomware and to investigate and prosecute cybercrime. Other facets of the cyber-related challenges facing DOJ are safeguarding sensitive and classified data and strengthening its information technology (IT) systems. In order make these things possible, the Department needs to recruit and retain cyber talent.

Responding to Known, Evolving, and Novel Threats

The Department faces the challenge of leveraging law enforcement, legal, IT, and intelligence resources to bring perpetrators of cybercrime to justice while also protecting the privacy of everyday Americans and engaging in lawful cybersecurity practices. To better position itself to respond to these challenges, the Department has launched a strategic cyber review.

Threat of a Cyber Supply Chain Attack

Cyber supply chain attacks are a significant concern to the Department. For example, in December of 2020, the FBI made a joint statement along with the Cybersecurity and Infrastructure Security Agency and the Office of the Director of National Intelligence about a significant cyber threat to users, including DOJ and other federal agencies, of the SolarWinds Orion incident, which was attributed to the Russian Foreign Intelligence Service (SVR). Also in December 2020, the U.S. Government Accountability Office (GAO) released a report assessing cyber supply chain management that identified 7 practices for providing an agency-wide approach to managing supply chain risks and made a total of 145 recommendations to 23 agencies to fully implement these foundational practices in their organization-wide approaches. The GAO found that none of the agencies it reviewed, including DOJ, had fully implemented all of the practices.

Recently, the Office of the Inspector General (OIG) initiated an audit of DOJ's cyber supply chain risk management efforts. The objectives of this audit are to determine the extent to which the Department, through the Justice Management Division and the Federal Bureau of Investigation (FBI), implemented an organizational supply chain risk management program that identifies, assesses, mitigates, and responds to supply chain risk throughout the IT lifecycle. Carefully reviewing and considering GAO's recommendations, as well as the OIG's upon the completion of our audit, will assist the Department in addressing this challenge.

Threat of Ransomware

Another threat to the Department, as noted by Deputy Attorney General Lisa Monaco in her remarks on June 7, 2021, are ransomware attacks,[3] which have increased in both scope and sophistication in the last year and pose a threat to U.S. national and economic security. As a result of this threat, the Department has provided guidance for ransomware and digital extortion investigations and recently launched a Ransomware and Digital Extortion Task Force to help bring the full authorities and resources at its disposal to confront the issue of ransomware and digital extortion. This year, DOJ investigators successfully seized $2.3 million in cryptocurrency paid to the

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

Colonial Pipeline attackers in a successful operation. This evolving threat is substantial, and the joint DOJ and the U.S. Department of Homeland Security ransomware resource, StopRansomware.gov, announced in July 2021, is a positive step toward raising awareness to defend against it. The challenge for the Department is to continually develop innovative approaches to defend against the technologically sophisticated and innovative bad actors who deploy destructive ransomware attacks.

Cybersecurity and Infrastructure Security Agency (CISA) ransomware awareness campaign
Source: CISA

Emerging Technology

Technology is everchanging and therefore presents an evolving threat landscape and additional challenges for the Department. New technologies such as artificial intelligence, unmanned aircraft systems or drones, cryptocurrencies, new encryption technologies, and 3-D printed firearms also present a new challenge for the Department.

Evolving 3-D printing technology is making it both more affordable and capable to print lethal firearms. This technology is therefore poised to provide an opportunity for prohibited individuals to make weapons that are undetectable by metal detectors and lack serial numbers, making them effectively untraceable. In light of this emerging technology challenge for the Department, the OIG is auditing the Bureau of Alcohol, Tobacco, Firearms and Explosives' (ATF) monitoring of 3-D firearm printing technology. The purpose of the audit is to evaluate the effectiveness of ATF policies and procedures regarding the monitoring and mitigation of risks presented by 3-D firearms printing technology and trafficking.

Among the continuing technology challenges for the Department is illegal activity on the dark web, including the use of cryptocurrencies for criminal transactions, which presents ongoing challenges to U.S. law enforcement agencies and their international partners. In December 2020, the OIG released a report on the FBI's strategy and efforts to disrupt illegal activities on the dark web. Among the issues identified in the report was the challenge of how the Department can most effectively utilize finite resources to investigate cryptocurrency on the dark web. According to the FBI, investigations involving the illicit use of cryptocurrency have increased from 15 cases in 2015 to over 350 cases in 2019 and resulted in the seizure of over $100 million in cryptocurrency. We found that rising costs of cryptocurrency support for dark web investigations, particularly licensing costs for analytic tools, and static funding from the Assets Forfeiture Fund resulted in disagreement between two FBI teams on the prioritization of resources and revealed concerns that they are conducting redundant work. The OIG recommended that the FBI complete its development of the FBI-wide cryptocurrency support strategy to better address this emerging technology challenge. This strategy is still in progress as of September 2021.

In light of the growing predominance of cryptocurrency in illegal Internet activities and the corresponding increase in cryptocurrency seizures, this emerging technology also presents the challenge of adapting traditional

[3] Ransomware is malicious software that denies access to a user's data by encrypting the data followed by cyber actors demanding a ransom to restore access to that data.

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

methods for managing seized assets. In recognition of this challenge, the OIG has initiated an audit to evaluate the U.S. Marshals Service (USMS) management of seized cryptocurrency. The audit will assess the effectiveness of USMS's policy and procedures for safeguarding, tracking, storing, valuing, and disposing of seized virtual currencies in its custody; and evaluate the USMS's plans to use a contractor to manage seized cryptocurrency.

Further, the growing role of emerging technologies in international criminal enterprises caused Congress to task GAO with studying human trafficking and the role that artificial intelligence, cryptocurrency, and online marketplaces, among other emerging technologies, play in trafficking.

Challenges Investigating and Prosecuting Cybercrime

The Department has several challenges to overcome when prosecuting and investigating cybercrime, including determining jurisdiction of the crime and offender, underreporting of incidents, lengthy and expensive investigations, evidence preservation, encryption, money laundering, and tracking digital currency. In addition, the sheer number of allegations related to these crimes continues to increase. According to an FBI press release, there were 791,790 complaints of suspected Internet crime in 2019, with an estimated loss of $4.2 billion dollars, and over the last 5 years, the FBI's Internet Crime Complaint Center reports that over 2.2 million complaints were reported to it with estimated losses totaling over $13.3 billion. According to the FBI, the highest incidents of Internet crime in 2020 were phishing scams, non-payment/non-delivery scams, and extortion.

Partnerships

Another challenge that the Department faces in investigating cyber threats is forming partnerships with private sector entities, state and local law enforcement, other federal agencies, and international law enforcement counterparts, including the International Criminal Police Organization (INTERPOL). As FBI Director Christopher Wray noted in his remarks at a September 2020 cybersecurity summit, cybersecurity requires "an enterprise approach—one that involves government agencies, private industry, researchers, and nonprofits, across the U.S. and around the world." In order to combat this issue, the FBI leads the National Cyber Investigative Joint Task Force, bringing together 30 co-located agencies from the Intelligence Community and law enforcement to develop a whole-of-government approach. A prior OIG audit of an FBI cyber initiative found that both FBI and the private sector found that information sharing remained a challenge, and we therefore recommended that the FBI expand private sector outreach to develop an environment that promotes information sharing and collaboration. With an increase in cybercrime and the growing complexity and international nature of such activity, it is important for DOJ to continue to maintain and develop further robust partnerships worldwide.

Technological Tools

The Department also faces the challenge of appropriately using technological tools to overcome challenges presented in investigating cybercrime. One continuing challenge the Department faces when investigating cybercrime is the use of encryption communication tools. Encryption is the process of hiding information by encoding it and only allowing someone with a key to unlock that code to access the information. Encryption presents an increasing challenge for Department law enforcement components, both in terms of their ability to access encrypted information relevant to a criminal investigation and because of the civil liberties and privacy issues presented.

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

Another tool presenting a challenge is the use of facial recognition technology, which can be used to help improve overall safety, protect critical infrastructure, and make criminals' online activity harder to conceal. However, the technology has raised many privacy concerns, including that it may be used without a subject's knowledge or consent, and has been subjected to increased criticism by non-law enforcement organizations, which have raised issues related to potential bias and perceived misuse by government.

The challenges facing federal agencies was highlighted in a recent GAO review of facial recognition technology. It found that there are various types of uses of facial recognition technology among 42 government agencies and that there is no common policy to govern its usage. The GAO made 2 recommendations to 13 federal agencies, including the DEA, FBI, and ATF, to implement a mechanism to track what non-federal systems are used by employees and assess the risks of using these systems. Implementing GAO's recommendations would assist the Department in addressing some of the challenges presented in using advancing technology.

Strengthening the Department's Cyber Capabilities and Defenses

Persistent and increasingly sophisticated cyber actors can disrupt, degrade, or destroy American economic, socio-cultural, and political interests. To continue to strengthen its cybersecurity posture, the Department faces multiple challenges, including enhancing its coordination and information-sharing, safeguarding data, and enhancing its cybersecurity physical and human capital infrastructure.

To assess DOJ's response to these challenges, the OIG recently initiated a review of the Department's efforts to coordinate the sharing of information related to combatting malign foreign influence in U.S. elections. This review will assess the effectiveness and resilience of the Department's information-sharing system; evaluate the Department's oversight, management, and coordination of its activities to respond to malign foreign influence on elections; and identify any gaps in or duplication of its information sharing efforts.

DOJ also faces the challenge of continuing to implement requirements outlined in the EO 14028, Improving the Nation's Cybersecurity. For example, Section 3 of the EO requires federal agencies to advance towards a Zero Trust Architecture, a security model that eliminates implicit trust in any one element, node, or service and requires continuous verification of the operational picture via real-time information from multiple sources. DOJ will need to invest in both technology and personnel to match these modernization goals. Another facet of the challenge the Department faces regarding its cybersecurity infrastructure is its need to improve its management of IT acquisitions and operations, something that the GAO identified in its March 2021 high-risk series update and an April 2021 study. The Department has recently taken steps to strengthen its ability to respond to cyber threats related to IT acquisitions.

Safeguarding Data and Information Systems

The Department has a responsibility to appropriately safeguard its data and information systems, which contain many different categories of sensitive data, including information that is personally identifiable, law enforcement sensitive, and classified. DOJ therefore needs to continue to prioritize efforts to safeguard the large volume of classified, law enforcement sensitive, and privacy protected information stored, transmitted, or

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

accessed by DOJ personnel every day. The Federal Information Security Modernization Act (FISMA) requires each federal agency to develop and implement an agency-wide information security program. Throughout Fiscal Year (FY) 2020, as required by FISMA, the OIG continued to assess the effectiveness of DOJ's information security program and practices. In FY 2020, the OIG assessed many different component-specific information systems, including those belonging to ATF, Civil Rights Division, FBI, Justice Management Division, National Security Division, and USMS. A majority of the FY 2020 FISMA audits led to at least one recommendation designed to strengthen component-specific information systems.

The onset of the Coronavirus Disease 2019 pandemic presented the Department with an unexpected challenge, as the number of its employees working remotely increased exponentially. The sudden shift to remote work and corresponding increase in the use of remote-access software created additional data and information system vulnerabilities. The OIG's ongoing FISMA FY 2021 audits include an assessment of vulnerabilities created or exacerbated by DOJ's use of remote-access software to facilitate telework during the pandemic, and whether any such vulnerabilities were effectively mitigated.

Recruitment and Retention of Cybercrime Focused Prosecutors, Analysts, and Agents to Address Human Capital Weaknesses

The Department is facing an increased need for qualified cybersecurity professionals, but hiring, retaining, and training cybersecurity professionals has been a longstanding challenge in the federal government. As the Department continues to strive to adapt to the rapidly changing cybersecurity world, it continues to recognize the importance of strengthening the workforce. The interagency Chief Information Officer Council examined the primary challenges facing the federal IT workforce and highlighted them in the Future of Federal IT Workforce Update (Workforce Update). The Chief Information Officer Workforce Update outlines five pillars of an effective federal IT workforce, which include recruitment and hiring, retention, training, augmenting, and measuring success. Additionally, the report stated that all IT workers require some security knowledge and protections such as the basic sharing of unclassified documents all the way to defending the nation's critical IT assets. More recently, in an effort to recruit prosecutors and attorneys equipped to handle emerging national security and criminal cyber threats, the Department announced the creation of a new Cyber Fellowship program, which will provide selected attorneys experience combatting these threats. Fellows will be rotated through multiple department components and handle a broad range of cyber cases and gain a comprehensive understanding of the Department's response to emerging and critical threats.

FBI Cyber Division personnel
Source: FBI

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

Because IT work has a security and protection function and also requires specialized legal expertise, it is critical that the Department continue to recruit, retain, and train IT and legal experts in cybersecurity to ensure continued protection from future cyber-related incidents.

Strengthening Community Engagement, Law Enforcement Coordination, and the Response to Violent Crime

The Department of Justice (DOJ or the Department) has consistently considered combatting violent crime as a significant priority. Just as consistently, strengthening police-community relationships, compiling timely and accurate data, fostering increased coordination and information-sharing, and performance-based metrics have proven to be important components of a successful strategy to reduce the effects of violence in communities. These areas continue to present challenges for the Department.

Enhancing Trust in Police-Community Relationships

A pressing challenge facing the Department is how to strengthen trust between the police and communities. Enhancing trust is critical because a constructive relationship between the police and the communities they serve is essential to effective policing. This is not a new challenge. In last year's Top Management and Performance Challenges (TMPC) report, the Office of the Inspector General (OIG) identified strengthening public confidence in law enforcement and protecting civil liberties as a challenge and, in the TMPC reports from 2015-2018, the OIG also identified building trust and improving police-community relations as a challenge.

Frisco, Texas, police officer shakes hand of community member.
Source: Community Oriented Policing Services Photo Contest; Kelly Clark; Courtesy of Frisco (TX) Police Department

The Department has recognized the importance of the public's trust. In May 2021, the Department announced a violent crime reduction strategy and identified enhancing public trust and legitimacy as one of the strategy's foundational principles. The Presidential Commission on Law Enforcement recognized in its December 2020 final report that "[t]here are grave consequences when communities lose their trust in law enforcement" and that "[m]uch work remains for law enforcement to optimize community trust and to improve practices." This finding is significant because, as the OIG noted in last year's TMPC report, the Commission was criticized for its lack of input from key stakeholders, including civil rights groups and police reform advocates.

As discussed in last year's TMPC report, the Department can build and maintain the public's trust in law enforcement at all levels—federal, state, and local—in several ways, including leading by example, addressing civil right violations by police, and grants and technical assistance that improve the relationship between police and communities. Additionally, body worn cameras (BWC) are an important tool that can increase transparency and accountability and, thus, can assist in fostering a positive relationship between the police and communities. Prior to June 2021, as detailed in the OIG's audit of the Department's BWC program, DOJ had no policy governing BWC use or BWC programs in place for its own law enforcement agencies. In June 2021, shortly before the OIG's audit report was publicly released, Deputy Attorney General Lisa Monaco issued a memorandum requiring components to develop and submit BWC policies for approval and implementation. In September 2021, the Department announced the launch of its first phase of BWC implementation beginning with two Bureau of Alcohol, Tobacco, Firearms and Explosives field divisions. The Drug

Strengthening Community Engagement, Law Enforcement Coordination, and the Response to Violent Crime

Enforcement Administration (DEA), Federal Bureau of Investigation (FBI), and U.S. Marshals Service (USMS) will also introduce the first phase of their use of BWC in pre-planned law enforcement operations. Also in September 2021, the Executive Office for U.S. Attorneys (EOUSA) hosted a national BWC training, which provided background on the new Department policy and DOJ agency perspectives, as well as training in the areas of discovery, victim issues, intake/charging, and use of BWC evidence in court. The Department can set an example for use of BWC by establishing successful programs that engender public trust.

The Department can also lead by example in other areas beyond the use of BWC. For example, in September 2021, the Department announced a Department-wide policy that limits circumstances in which federal law enforcement can use certain physical restraints and entry techniques. The Attorney General recognized that this new policy, combined with the expansion of the use of BWC, "are among the important steps the department is taking to improve law enforcement safety and accountability."

While the overwhelming majority of law enforcement officers are dedicated public servants, who make great sacrifices to protect their communities, the Department has tools it can deploy to assist in building trust between law enforcement and the communities they police by appropriately and effectively seeking accountability in those instances when systemic or individual abuses occur. For example, under 34 U.S.C. § 12601 (formerly 42 U.S.C. § 14141), the Civil Rights Division (CRT) is empowered to investigate law enforcement agencies for patterns or practices of unconstitutional policing and bring civil actions. To that end, in April 2021, the Department announced an investigation of the City of Minneapolis, Minnesota, and the Minneapolis Police Department that will assess, among other things, all types of force used by the police department's officers and whether the police department engages in discriminatory policing. In April 2021 and September 2021, the Department released internal guidance that sets out principles to guide the Department's use of consent decrees and monitorships with police departments. In addition, the Department's CRT can seek to hold individuals accountable through prosecution for criminal violations of civil rights statutes. The monumental challenge for the Department in this context is to continue to support the essential work of law enforcement officers who selflessly, effectively, and even-handedly serve their communities, while taking steps to protect the public from those officers who misuse their authority.

Finally, the Department can provide grants and technical assistance to local police that help to reduce violent crime while also improving police-community relationships. In its May 2021 violent crime strategy memorandum, the Department recognized the role of grants in helping reduce gun violence and violent crime "[b]y funding research, investing in prevention and intervention programs, and supporting state and local officials through training and technical assistance." The Department's grantmaking components, such as the Bureau of Justice Assistance, the Office on Violence Against Women, and the Office of Community Oriented Policing Services (COPS Office) can also fund programs that help to grow the public's trust in law enforcement. The COPS Office offers several resources to help police departments build community trust, such as the Community Policing Development Program and the COPS Hiring Program. The Department can further enhance the public's trust in law enforcement, and address this challenge, by ensuring that it provides oversight and accountability regarding the use of federal funds by state, local, and tribal law enforcement agencies and other grant recipients. To that end, the Department recently directed its CRT and grant-making components,

Strengthening Community Engagement, Law Enforcement Coordination, and the Response to Violent Crime

including the COPS Office, to commence a review of the Department's implementation and administrative enforcement of Title VI of the Civil Rights Act of 1964 and the nondiscrimination provisions of the Omnibus Crime Control and Safe Streets Act that prohibit recipients of federal financial assistance from discriminating against any person on the basis of race, color, or national origin, among other bases.

Increased Coordination and Information-Sharing

Information sharing and coordination among federal, state, and local entities is essential in combating crime, particularly for complex domestic and international criminal activity, and remains a significant challenge for the Department. Unfortunately, a number of OIG reviews have identified significant issues that can arise when coordination and information sharing does not effectively occur. For example, in July 2019, the DOJ OIG and the U.S. Department of Homeland Security (DHS) OIG conducted a joint review examining law enforcement cooperation on the Southwest border between DOJ's FBI and DHS' Immigration and Customs Enforcement's Homeland Security Investigations (HSI), which identified cooperation failures between the FBI and HSI and factors that may have contributed to the failures. Among other things, the joint report found that the FBI and HSI had inconsistent practices, lacked specific policies, and many agents were unaware of requirements related to deconfliction of investigative targets and events. Further, DOJ and DHS do not have a memorandum of understanding related to cooperation on the Southwest border. Although the FBI has agreed with this recommendation and provided a response, HSI has not concurred and the recommendations remain open. More recently, the OIG's investigation and review of the FBI's handling of allegations of sexual abuse by former USA Gymnastics physician Lawrence Gerard Nassar found that FBI officials in multiple offices failed to expeditiously notify state and local law enforcement about the allegations, and other FBI field offices with stronger jurisdictional links to the allegations failed to mitigate the ongoing danger posed by Nassar. Additionally, the OIG's review of the Department's implementation of its Zero Tolerance Policy found that DOJ leadership did not effectively coordinate with the Southwest border U.S. Attorney's Offices, USMS, U.S. Department of Health and Human Services, or the federal courts prior to urging DHS to implement the practice of referring family unit adults to DOJ for prosecution. This lack of coordination resulted in, among other things, the Department failing to carefully and appropriately consider the effects of family unit prosecutions and child separations. The OIG recommended, among other things, that prior to issuing a significant policy affecting multiple Department components, other Executive Branch agencies, or the courts, that the Department coordinate directly with affected stakeholders to ensure effective implementation.

Sharing information in an effective way to eliminate gaps and provide value to an investigation and ultimately produce results is the key to reducing crime. This requires actions, such as information-sharing agreements, that result in better cooperation to foster better results in criminal investigations domestically and abroad, and it remains one of the more significant challenges facing the Department.

Strategic Management and Oversight of DOJ's Partnerships with Foreign Law Enforcement

As noted in its strategic plan, "DOJ has long recognized that the peace and security of the United States is strengthened by the development of professional foreign law enforcement partners that practice the most modern law enforcement techniques and respect and uphold the rule of law." The Department's ability to meet and defeat the growing threat posed

Strengthening Community Engagement, Law Enforcement Coordination, and the Response to Violent Crime

by transnational crime will require strategic management and robust oversight of DOJ's increasingly frequent interactions with foreign law enforcement partners.

A Thai police officer attends FBI-sponsored training in Chiang Mai, Thailand
Source: FBI

One of the Department's initiatives to combat global crime is focused on promoting the rule of law through grants and law enforcement training programs. DOJ must be careful to ensure that its expanding authorities in international arenas result in fully coordinated training and assistance with sufficient monitoring efforts. A recent report issued by the U.S. Government Accountability Office recommended that State Department, U.S. Agency for International Development, DOJ, and other agencies involved in providing rule of law assistance, coordinate their efforts effectively—including involving all relevant entities—because such coordination is key to providing assistance in an efficient and accountable way.

A second strategy to meet this challenge focuses on developing effective foreign law enforcement partners on whom the Department can rely to help target and disrupt transnational drug trafficking organizations impacting the United States. For example, the DEA relies on international partnerships, such as Sensitive Investigative Units (SIU) and Non-SIU Vetted Units (VU), to target and disrupt transnational drug trafficking organizations, conduct bilateral operations, coordinate Judicial Wire Intercept Programs, and gather intelligence on illicit drug smuggling into the United States. According to its most recent budget request, the DEA works with over 900 SIU members. While the DEA's activities with its foreign partners are integral to the DEA's global operations, the DEA's involvement with and funding of foreign law enforcement units in areas known for pervasive corruption can pose significant risks to DEA personnel, information security, the safety of U.S. and foreign civilians, and diplomatic relations. It can also undermine the DEA's and Department's ability to meet the challenge of addressing transnational crime.

These problems were highlighted in an August 2021 OIG report that evaluated the effectiveness of the DEA's headquarters-based oversight of DEA-supported foreign law enforcement units, including SIUs, VUs, and other less-structured initiatives. During the audit timeframe of Fiscal Years (FY) 2017-2019, the DEA had SIUs in 15 countries, VUs in 8 countries, and numerous other partnerships throughout the world. The OIG found that headquarters-based management and oversight of supported law enforcement units was insufficient for the high-risk environment in which the units operate. In addition, the DEA lacks a comprehensive strategy for these programs, which impedes its ability to make well-informed decisions, effectively manage its foreign partnerships, and demonstrate the collective success of DEA-supported operations. The OIG made 10 recommendations designed to improve, among other things, the DEA's reporting and tracking of critical incidents involving DEA-supported foreign law enforcement units, written policies and protocols, and tracking and assessing performance. Additionally, the OIG recommended the DEA conduct a comprehensive risk assessment of DEA's efforts to provide assistance to foreign law enforcement units.

Strengthening Community Engagement, Law Enforcement Coordination, and the Response to Violent Crime

As the threat of transnational crime continues to increase, the Department will continue to need to engage with foreign law enforcement partners more frequently. It will remain a challenge for the Department to ensure that interactions and relationships with foreign law enforcement partners are effectively managed and appropriately overseen.

Effective Coordination and Evidence-Sharing with Foreign Partners

Coordinating and sharing evidence with foreign authorities is critical to protecting Americans against serious crimes, including transnational criminal organizations, violent gangs, drugs, cybercrime, child exploitation, corruption, fraud, and money laundering. Accordingly, the Department must continue to address the challenges associated with effectively coordinating with foreign partners to protect against and solve serious crimes.

Mutual legal assistance (MLA) requests are one of the most widely used mechanisms for acquiring information and evidence internationally in criminal investigations and prosecutions, including witness statements, sworn testimony, and business records of entities located outside the requesting country. MLAs have become increasingly important to law enforcement as criminal activity more frequently crosses international borders. Given the increased number of incoming MLA requests from foreign countries, rising caseloads, and forthcoming responsibilities pursuant to agreement under the Clarifying Lawful Overseas Use of Data Act, a significant challenge for the Department is ensuring that the Criminal Division's Office of International Affairs' (OIA) can meet these growing demands. In July 2021, the OIG released a report that examined OIA's management of MLA requests from foreign law enforcement authorities. The OIG found that OIA is making progress in improving its process for handling incoming MLA requests but continues to be challenged by at least three main areas: (1) the high pending caseload, (2) hiring and retaining employees, and (3) an antiquated case management system. Meeting this challenge is particularly important because the failure to effectively do so could undermine the United States' ability to obtain assistance from foreign countries in critical matters involving, among others, national security, human trafficking, and information security.

Continued Efforts to Reduce Gun Violence and Other Violent Crime

As the chief federal law enforcement agency, the Department has an important role in coordinating violent crime reduction efforts across the country. This role is particularly important because of the increase in violent crime in 2020 and early 2021. According to data released by the FBI in September 2021, the number of murder and nonnegligent manslaughter offenses in 2020 increased 29.4 percent, and the overall violent crime rate rose 5.2 percent when compared with the 2019 rate, which is the first increase in 4 years. The Attorney General has said that "[p]rotecting our communities from violent crime is a top priority for the Department of Justice" due to the "deeply troubling" increase in gun and violent crime.

In May 2021, the Department outlined a strategy to address gun violence and other violent crime through fostering trust and legitimacy in the communities the Department serves; investing in community-based prevention and intervention programs; setting strategic enforcement priorities; and measuring the results of the Department's efforts. To implement these principles, the Department announced that it will increase intradepartmental coordination, strengthen the Project Safe Neighborhoods (PSN) nationwide violent crime reduction program, review grant-making

Strengthening Community Engagement, Law Enforcement Coordination, and the Response to Violent Crime

support for violent crime reduction efforts, and align the efforts of Department law enforcement agencies. Since its inception in 2001, PSN has been shown to be an effective tool for reducing gun and gang crimes across the United States at the state and local levels. Communities with PSN programs experienced significant reductions in violent crime as compared to other locations that did not have PSN interventions. To further support the implementation of its violent crime reduction strategy, the Department launched five cross-jurisdictional strike forces to help reduce gun violence by disrupting illegal firearms being trafficked from source cities, through other communities, and into five key market regions: (1) New York, (2) Chicago, (3) Los Angeles, (4) San Francisco Bay Area/Sacramento Region, and (5) Washington, D.C.

The Department's challenge will be to effectively implement these programs to achieve measurable results on a national scale. It is imperative that the Department monitor the data and support community-based adjustments to the crime prevention and violence reduction approaches as warranted by the empirical evidence. This performance management-based focus is an ongoing challenge for the Department and is critical to the success of its strategy to reduce violent crime.

Continued Improvement of Crime Data Collection Efforts

Complete, timely, and accurate data about crime can assist the Department in assessing its law enforcement efforts to address violent crime. For example, the collection of data about crimes committed throughout the country can help combat violent crime by guiding the Department in determining where it should devote its resources. Therefore, the Department's role in collecting and maintaining accurate data about crime is critical to a crime reduction strategy. However, it also has proven to be a significant challenge for the Department.

The FBI's Uniform Crime Reporting (UCR) Program serves as the national repository for crime data collected and submitted by law enforcement. While federal law requires that federal law enforcement agencies provide information to the UCR, participation of state and local agencies is voluntary and difficulties in obtaining crime data persist. In its FY 2021 budget request and authorization, the FBI described "the need to generate a pathway to greater crime data collection and to improve the nation's crime statistics for reliability, accuracy, accessibility, and timeliness, and to expand the depth and breadth of data collected." To that end, as of January 2021, the Department's crime data is being collected through a National Incident-Based Reporting System (NIBRS) and the legacy Summary Reporting System has been retired. In recognition that participation with NIBRS needs to be increased, according to the FBI, "the UCR Program is partnering with the Bureau of Justice Statistics on the National Crime Statistics Exchange, working with advocacy groups to emphasize the importance of NIBRS data, and transitioned the UCR Program to a NIBRS-only data collection." According to the FBI, NIBRS can provide more useful statistics to promote constructive discussion, measured planning, and informed policing. Ensuring the successful transition to NIBRS and increasing voluntary participation are critical to DOJ's ability to use data to address crime.

The OIG has previously identified challenges that the Department faces in its collection of reliable, complete, and timely crime data specifically in the context of the Department's tribal law enforcement efforts pursuant to the Tribal Law and Order Act of 2010 (TLOA). A 2017 review to assess DOJ's progress in implementing TLOA requirements found that crime data in

Strengthening Community Engagement, Law Enforcement Coordination, and the Response to Violent Crime

Indian country remains unreliable and incomplete, which limits the Department's ability to engage in performance based management of its efforts to implement its TLOA responsibilities. We found that this crime data deficiency was due to that fact that more than 7 years after the enactment of TLOA, DOJ's Bureau of Justice Statistics was still developing its process for collecting and analyzing data about crimes in Indian country. The OIG also found limitations in EOUSA's and the FBI's TLOA data, which is collected to meet TLOA reporting requirements, and that EOUSA, the FBI, and Bureau of Justice Statistics did not effectively analyze the data they collect. To improve crime data collection and performance-based management of law enforcement activities in Indian country, the OIG recommended that EOUSA and the FBI analyze available data to identify the law enforcement needs, and provide training to all staff responsible for Indian country data collection to ensure data is captured uniformly. As of September 2021, there is one remaining open recommendation from this review, which called for the Department to update policy memoranda to U.S. Attorneys and heads of components to incorporate TLOA mandates.

The Department's ability to use crime data depends on the accuracy of the data collected and, thus, it will continue to be a challenge for the Department to encourage voluntary reporting of crime data.

Managing the Opioids/Fentanyl Crisis

Given the Department of Justice's (DOJ or the Department) law enforcement responsibilities and the Drug Enforcement Administration's (DEA) role as a regulator of controlled substances, the widespread misuse of and addiction to opioids—including fentanyl, a powerful synthetic opioid that is similar to morphine but 50 to 100 times more potent—is a significant challenge for the DEA and the Department given the ongoing national crisis affecting public health and the social and economic welfare of the country. According to data from the Centers for Disease Control and Prevention (CDC), from 1999 to 2019, nearly 500,000 people died from drug overdoses involving opioids. Moreover, the CDC estimates that the annual cost of prescription opioids abuse in the United States, which is just a portion of all opioids/fentanyl abuse, is $78.5 billion, which includes healthcare costs, addiction treatment, criminal justice involvement, and loss of productivity. The DEA's 2020 National Drug Threat Assessment found that the "opioid threat (controlled prescription drugs, synthetic opioids, and heroin) continues at ever-increasing epidemic levels, affecting large portions of the United States." According to the DEA, fentanyl and other synthetic opioids continue to be the most lethal controlled substances. The continuing challenge of confronting the opioids crisis has been heightened by the impact of the Coronavirus Disease 2019 (COVID-19) pandemic on drug abuse and overdose deaths.

Increased Opioids and Fentanyl-Related Deaths

Fentanyl is a significant contributor to the rates of overdose deaths observed across the country. According to provisional drug overdose death data issued by the CDC's National Center for Health Statistics, in 2020 there were 92,476 drug overdose deaths reported, which is a 30 percent increase from the 71,130 deaths reported in 2019. According to the CDC, opioids were involved in over 70 percent (49,860) of all drug overdose deaths in 2019. In December 2020, the CDC issued a Health Alert Network Advisory noting "a concerning acceleration of the increase in drug overdose deaths, with the largest increase recorded from March 2020 to May 2020, coinciding with the implementation of widespread mitigation measures for the COVID-19 pandemic." According to the CDC, the large increase in overdose deaths in that time frame was due to a rise in synthetic opioids deaths, which the CDC said likely involved illicitly manufactured fentanyl.

Coordinating the Department's Response

As the nation's leading law enforcement agency and supporter of local law enforcement efforts, the Department has a major role to play in coordinating a national response to the opioids and fentanyl crisis. As the Office of the Inspector General (OIG) noted in last year's Top Management and Performance Challenges report, responding to this urgent national emergency is one of the significant challenges that the Department continues to face. At the Department's 2020 National Opioid Summit, then-Deputy Attorney General Jeffrey Rosen detailed several initiatives to combat the crisis, including increased law enforcement operations such as Operation

U.S. Marshals examine seized drugs during Operation Frontier Justice
Source: U.S. Marshals Service

Managing the Opioids/Fentanyl Crisis

Synthetic Opioid Surge or S.O.S. This effort focuses on controlled opioids in 10 federal judicial districts located in California, Kentucky, Maine, New Hampshire, Ohio, Pennsylvania, Tennessee, and West Virginia with the highest overdose death rates in the country. The strategy calls for prosecution of all readily provable cases involving synthetic opioids and taking investigative steps to identify wholesale distribution methods. In addition, the Department has created regional task forces and utilized civil injunctions to address wrongdoing in the prescription opioids supply chain. More recently, the DEA issued a public safety alert warning that international and domestic criminal drug networks are increasingly flooding the United States with lethal counterfeit pills that are made to look like prescription opioids and are widely accessible and often sold on social media and e-commerce platforms, making them available to anyone with a smartphone, including teens and young adults. As of September 2021, more than 9.5 million counterfeit pills were seized for the year, which is more than the last 2 years combined.

In addition to these efforts, there are areas in which the Department's response could be strengthened. For example, in a report issued in 2019 regarding the DEA's response to the opioids crisis, the OIG found that DEA policies and regulations did not adequately hold registrants accountable or prevent the diversion of pharmaceutical opioids. The OIG made nine recommendations to improve the Department's and the DEA's ability to combat the diversion of pharmaceutical opioids and effectively regulate registrants that engage in diversion. One of the recommendations was that the DEA develop a national prescription opioids enforcement strategy that encompasses the work of all DEA field divisions tasked with combating the diversion of controlled substances and establish performance metrics to measure the strategy's progress. As of September 2021, this recommendation and three others remain open. Progress on these open recommendations will aid in the DEA's and Department's efforts to address the challenge presented by the opioids crisis.

Community-Based Strategies

Beginning in 2016, the DEA developed and deployed a "360 Strategy," which it deployed in 23 pilot cities fraught with opioids issues. The DEA described the strategy as "an innovative three-pronged approach to combating heroin/opioid use through Law Enforcement, Diversion, and Community Outreach." The law enforcement prong of the strategy targeted the most significant drug trafficking threats, while the diversion prong leveraged the DEA's regulatory authority to prevent non-medical abuse of controlled prescription drugs. The community outreach prong aimed to help communities prevent a resurgence in drug trafficking after an enforcement operation by using a comprehensive public messaging program and creating a grassroots movement to create a safer community.

Drugs being turned in during National Prescription Drug Take Back Day
Source: DEA

In February 2021, the DEA initiated Operation Engage, which builds on and replaces the 360 Strategy by using community based strategies to address

Managing the Opioids/Fentanyl Crisis

the illicit narcotics that present the greatest threat to public health in different communities, rather than focusing solely on opioids. Through this program, each DEA Division focuses on a designated city or region, identifies its local drug-related enforcement priorities, supports local drug use prevention efforts, and serves as a bridge between public safety and public health efforts to decrease illegal drugs.

In September 2020, the OIG conducted an audit of the DEA's community-based efforts to combat the opioids crisis and concluded that the program helped increase awareness of opioids-related issues, provide training, build anti-drug coalitions, and create and distribute educational materials made available for no charge. The OIG also identified areas for improvement in the DEA's pilot city selection process, allocation of resources, and collaborative efforts with other federal entities tasked with combatting the opioids crisis. We also found that the DEA lacked an outcome-oriented performance measurement strategy to assess the effectiveness of its community outreach efforts. The OIG's recommendations will help the Department improve its collaboration with federal partners and implement a performance-based approach to maximize the impact of its community-based intervention programs.

Grants to Support Opioids Programs and Law Enforcement Efforts

The Department also plays an important role in supporting the state and local response to the opioids and fentanyl crisis through its grant awards. For example, in October 2020, DOJ announced it had awarded over $341 million in grants, adding to an already unprecedented level of Department investment targeted at fighting this national crisis. A significant portion of this grant funding (more than $147 million) was awarded to support the Bureau of Justice Assistance's Comprehensive Opioid, Stimulant and Substance Abuse Site-based Program (COSSAP), which is designed to provide financial and technical assistance to state, local, and tribal governments to develop, implement, or expand comprehensive intervention efforts for individuals impacted by opioids and other illegal drugs. One of the Department's biggest challenges in this area is ensuring that the funding it provides is accomplishing the goals of its grant programs. The OIG has an ongoing audit of COSSAP examining whether the Bureau of Justice Assistance implemented adequate oversight of COSSAP, coordinated with COSSAP partners and stakeholders, and accomplished COSSAP objectives and deliverables. The OIG also has an ongoing audit of the Office of Community Oriented Policing Services' (COPS Office) Anti-Heroin Task Force Program, which is assessing the COPS Office administration and oversight of the program, determining the extent to which the program has been successful, and reviewing coordination efforts between the COPS Office and other DOJ entities to combat the heroin and opioids crisis.

Fentanyl Scheduling

The DEA has concluded that fentanyl, which is involved in more deaths than any other controlled substance, is the primary driver of the current crisis. According to the DEA, fentanyl is smuggled into the United States primarily in powder and counterfeit pill form. One of the significant challenges facing the Department and the DEA is categorizing for DEA control, also known as scheduling, fentanyl-related substances under the Controlled Substances Act. Using his temporary scheduling authority under the Controlled Substances Act, in 2018, then-Attorney General Jeff Sessions classified all fentanyl-related substances under Schedule I, which are substances that have a high potential for abuse; no currently accepted medical use in treatment in the United States; and are not safe for use under medical supervision. However, there has been opposition to this class-wide

Managing the Opioids/Fentanyl Crisis

scheduling by organizations that were concerned that such action would "exacerbate pretrial detention, mass incarceration and racial disparities in the prison system." Additionally, according to the Congressional Research Service, the medical utility of many of the substances subject to the DEA's class-wide scheduling (which potentially encompassed thousands of different chemicals) is unknown. This temporary scheduling was extended by Congress, but only through January 28, 2022, by the enactment of the Extending Government Funding and Delivering Emergency Assistance Act.

Fentanyl is a potent synthetic opioid
Source: DEA

In April 2021, the U.S. Government Accountability Office published a report addressing the issue of classifying all fentanyl-related substances under Schedule I, which it noted has potential effects on drug classification, research, and law enforcement. The U.S. Government Accountability Office identified a tension in such an approach because broadly classifying all fentanyl-related substances as Schedule I may serve the law enforcement interest in deterring creation of new, potentially dangerous substances, but may come at the expense of, among other things, impairing medical research. DOJ and the DEA face the challenge of reaching a resolution with policymakers on these conflicting concerns and adapting its approaches to the policy environment after the temporary fentanyl scheduling expires in January 2022 and thereafter in response to potential legal developments.

The tragedies arising from the opioids crisis place a heavy burden on the DEA and the Department to act with urgency to resolve the time-sensitive challenge of determining which will be the best course of action, both to enable successful law enforcement action with respect to fentanyl and related substances, and to address the concerns of other stakeholders.

Managing Human Capital

The Department of Justice (DOJ or the Department) faces an array of human capital challenges, several arising from the pandemic, including keeping employees and visitors safe, updating workplace flexibilities, reconfiguring the physical workspace, and modernizing information technology (IT) infrastructure. Because the success of the Department's mission is driven by the quality of its personnel, we focus on the human capital aspect of these challenges. Given that there is no one-size-fits-all solution to manage each component's issues, one challenge facing the Department is providing guidance on human capital issues that is sufficiently flexible to allow each component to address its business needs in a manner that is responsive to the concerns and needs of its employees. DOJ continues to face the challenges of remaining competitive in the employment marketplace so that it can recruit and retain a highly skilled and diverse workforce. Many of those challenges have become more pressing as a result of the Coronavirus Disease 2019 (COVID-19) pandemic. The Department also faces the continuing challenge of ensuring a workplace that is free from sexual harassment and misconduct.

Human Capital and Safety Issues Arising from the Pandemic

The COVID-19 pandemic resulted in a seismic shift in how federal employees, including Department personnel, carried out their duties. According to 2020 Federal Employment Viewpoint Survey data, the percentage of federal employees who teleworked daily grew from 3 percent to 59 percent during the peak of the pandemic. As the federal government adapts to a work environment that continues to evolve as a result of the pandemic, the Department faces new human capital challenges.

A bandage placed on a patient's vaccine injection site
Source: Lauren Bishop, Centers for Disease Control and Prevention

The Department faces a host of health and safety issues related to returning to the workplace post-pandemic. To help federal agencies address return to work issues, in June 2021, the Office of Management and Budget (OMB), Office of Personnel Management (OPM), and General Services Administration issued a memorandum on planning for a safe increased return of federal employees and contractors to physical workplaces. In addition to addressing such issues as physical occupancy limits, vaccination status, and workplace flexibilities, the memorandum directed agencies to update their workplace safety plans. In July 2021, OMB released another memorandum that provided general guidance regarding workplace flexibilities, including telework, remote work, and work hours.

One way in which the Department responded to the pandemic was through increased availability and use of workplace flexibilities, such as telework, remote work, and flexible schedules. Although Department leadership has not yet announced post-pandemic policies governing workplace flexibilities, there appears to be strong support among DOJ employees for the continued use of enhanced workplace flexibilities. The Department faces the challenge of how to effectively leverage workplace flexibilities, something it acknowledged in June 2021 can increase productivity, as well as the challenge of how to provide guidance across the organization that can be adapted to each component's mission. When entering the post-pandemic

Managing Human Capital

work environment, the OMB, OPM, and General Services Administration memorandum advised federal agencies to establish guardrails for decision making, and to delegate to "the lowest appropriate levels in the organization to provide maximum flexibility for defining work requirements to meet mission and workforce needs." DOJ has long lagged behind other federal agencies in allowing many workplace flexibilities. Although the mission and job requirements within some components preclude certain options, such as extensive telework and alternate work schedules, many DOJ components were forced during the pandemic to allow flexibilities that were previously unavailable. Maintaining those opportunities for certain categories of employees will likely enhance the Department's ratings in the 2020 Federal Employment Viewpoint Survey data and the Partnership for Public Service, which track levels of employee engagement and satisfaction on various scales, and which serve as indicators for the Department's ability to compete for and retain top quality personnel.

In an April 2021 limited-scope review, the Office of the Inspector General (OIG) found that the Executive Office for Immigration Review (EOIR) was unable to implement widespread telework for staff because of a lack of equipment, technological limitations, and the need to process mailed and in-person filings. In its response to the report, EOIR agreed that it was not in the best posture to respond to the pandemic because of limited equipment availability and software functionality and because it has historically been a paper-based agency. The OIG recommended that EOIR develop a plan to ensure maximum telework capability for all positions and staff in locations affected by the COVID-19 pandemic or in the event of a future pandemic or similar conditions. In addition, we recommended that EOIR ensure that it procures sufficient equipment and addresses software limitations to enable the broadest possible telework. EOIR concurred with these recommendations and said that it has procured additional IT equipment and software so that it will be better positioned in the future.

As fluctuations in the status of the COVID-19 pandemic arise, such as increasing infection rates in some locations across the county and complications from emerging variants of the virus, the Department will need to navigate a complex and changing landscape that impacts a host of human capital issues.

Recruitment, Retention, and Diversity

The wide availability of workplace flexibilities not only improve the Department's functionality during the pandemic and other emergencies, but they also increase the Department's ability to recruit and retain a highly qualified and diverse workforce. OPM has advised federal agencies that they "can leverage issues such as telework, remote work, and flexible work schedules as tools in their broader strategies for talent recruitment and retention, and for advancing diversity, equity, inclusion, and accessibility in the Federal workforce." Department leadership has recognized the role that workplace flexibilities can plan in recruitment, retention, and diversity of its workforce. As employees' pandemic-related conditions improve, the Department will face the challenge of maintaining the expanded level of workplace flexibilities while continuing to meet its important mission. Doing so will be critical to the Department's ability to recruit and retain the highly qualified, diverse, and engaged personnel necessary to accomplish the Department's work. Promoting diversity in the workforce is another continuing challenge for the Department. As recognized in Executive Orders (EO) 13583 and 14035 and in an OPM policy, a workplace that is diverse, equitable, inclusive, and accessible draws on the talents of all parts of society and brings a fuller array of perspectives to overcome challenges,

Managing Human Capital

which yields better results and leads to higher performing organizations. In 2018, the OIG completed a review of gender equity in the Department's law enforcement components, which assessed overall gender equity, based on both gender diversity in the workforce and employees' perceptions of gender equity and discrimination in the four law enforcement components. The OIG found, among other things, significant gaps in the number of females in criminal investigator and leadership positions, the number of female criminal investigators receiving promotions, and perceptions of gender equity among employees. The OIG recommended that all four components develop and implement recruitment, hiring, and retention strategies, address the barriers to advancement for women across all job types, and improve the objectivity and transparency of the merit promotion process. In response to the OIG's review, the four components examined potential barriers to gender equity through focus groups, surveys, analysis of various policies, workforce demographic data analysis, and promotion data analysis. The components also developed and implemented a number of initiatives to address the identified barriers to recruiting, hiring, promoting, and retaining women, that included branding and marketing recruitment campaigns that focused on social media outreach, issuance of more flexible work/life policies and headquarters rotation policies, and improving the transparency and objectivity of the Special Agent merit promotion processes. Two of the components reported improvements in the percentage of women that made up criminal investigator training classes and graduates.

While the above-described initiatives were developed to improve gender equity, they are also likely to contribute to improving diversity broadly in the workforce. Due to the impact of our gender equity report, the OIG initiated an examination of racial equity in the Department's law enforcement components, which remains ongoing. To further assist the law enforcement components and promote a diverse workforce, in this review the OIG will assess equity across race, color, national origin, and ethnicity by reviewing component demographics, recruitment, hiring, retention, attrition, promotions, and awards. This review will also include a survey assessing staff perceptions related to equity. Separately, the OIG is continuing its work on gender equity by reviewing the training and evaluation of new Special Agents and Intelligence Analysts at the FBI Academy. This ongoing review will examine policies and practices, trends and patterns for male and female Special Agent and Intelligence Analyst trainees, and perceptions of gender equity.

A U.S. Marshals academy class participates in training
Source: U.S. Marshals Service

Maintaining a Safe Workplace Environment Free from Sexual Harassment and Misconduct

As the federal agency with primary responsibility to enforce the nation's laws, including Title IV of the Civil Rights Act of 1964, Title VII of the Civil Rights Act of 1964 (with respect to state and local government employers), the Fair Housing Act, the Equal Credit Opportunity Act, and Title IX of the Education Amendments Act of 1972, it is imperative that the Department as an employer serve as a leader in maintaining a workplace free of sexual

Managing Human Capital

harassment and misconduct. The Department instituted a zero tolerance policy regarding sexual harassment in 1993, amended the policy in 1998, and reaffirmed it in 2015, after an OIG report revealed systemic issues within the Department's law enforcement components' processes for handling allegations of sexual harassment and misconduct. In addition to conveying the priority of that objective, the Department must respond promptly and appropriately to substantiated allegations of such misconduct. Doing so enhances the professionalism of the Department, supports victims, and deters the toxic misconduct that is antithetical to the Department's overall mission. The persistence of this issue arising throughout DOJ components, as evidenced by numerous recent OIG investigations, makes clear that this is a challenge that requires the continued vigilance of DOJ and component leadership.

For example, in January 2021, the OIG reported that a Federal Bureau of Investigation (FBI) Assistant Special Agent in Charge engaged in unwanted sexual touching with three FBI employees, created a hostile work environment by engaging in that unwanted physical sexual contact and making offensive sexual comments to FBI employees. The OIG found that this conduct violated the Department's zero tolerance policy regarding sexual harassment, as well as FBI policies regarding sexual harassment and employee conduct. In November 2020, the OIG found that an Assistant U.S. Attorney engaged in sexually harassing conduct by making sexually inappropriate comments to an intern, an Assistant U.S. Attorney, and two other individuals, and also by inappropriately touching the intern's breast. The OIG found that this conduct violated the zero tolerance policy and state law. These recent investigative findings are consistent with an increasing number of similar such allegations and findings against Department personnel over the past several years, summaries of many such investigations are reported on the OIG's Investigative Summaries page.

The Department has taken important steps to respond to prior OIG reports in this area. For example, in response to an OIG report issued in June 2017 identifying deficiencies in how the Civil Division handled sexual harassment and misconduct allegations, the Department established a working group to consider how to eliminate sexual harassment and more effectively respond to misconduct allegations. The effort led to issuance of new sexual harassment and misconduct directives in April 2018, which required thatall components have policies and procedures in place that ensure consistency in the imposition of discipline for substantiated allegations; ensure that employees are informed of all avenues for reporting allegations; develop a process for tracking allegations; ensure that all non-frivolous allegations are reported to the OIG; and develop a policy regarding awards and public recognition of employees subject to misconduct allegations or disciplinary actions.

More recently, in a memorandum issued to all DOJ employees in July 2021, Deputy Attorney General Lisa Monaco reaffirmed the Department's commitment to maintain a workplace free from sexual harassment and misconduct. Deputy Attorney General Monaco's memorandum stated it is "critical to our duty as principled defenders of the law to combat sexual harassment and misconduct in our own workplace and hold offenders accountable for their actions." In recognition of the need to provide a safe workplace and achieve gender equality, this memorandum announced that the Department was empaneling a Steering Committee to review sexual harassment policies and practices, training, and education across the Department. The Deputy Attorney General directed the committee to provide recommendations within 180 days to ensure that the Department's

Managing Human Capital

policies are consistent, cohesive, and effective in preventing sexual harassment and misconduct and meeting the needs of its workforce.

While the Department's recent actions are significant, addressing the issue of sexual harassment and misconduct is a pernicious issue that has presented a challenge for many years. The Department must be vigilant and continue to work to maintain a workplace that is both safe for its employees and a model for other employers.

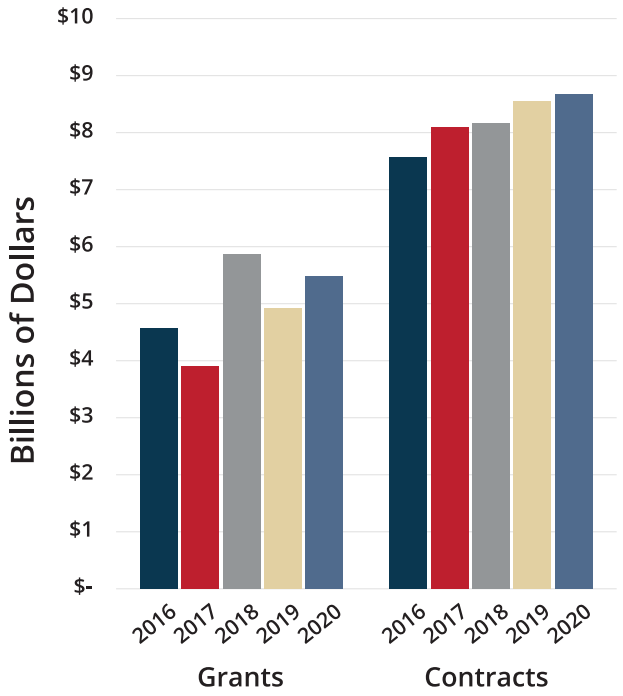
Human Resource Policies

An ongoing challenge, as noted above and in last year's Top Management and Performance Challenges report, is for the Department to recruit and retain a highly qualified and diverse set of employees and to remain competitive with other federal agencies. Accomplishing this goal requires current, complete, and consistent human resource (HR) policies fundamental to the Department's HR infrastructure and human capital management. As the OIG detailed in an August 2021 Management Advisory Memorandum issued to the Justice Management Division, the Department faces the challenge of ensuring that its HR policy includes pertinent HR guidance and contains information that is consistent with current relevant regulations and OPM guidance. Among other things, the OIG found that the Department lacks a centralized location for its HR guidance, and that the Department has not fulfilled its own internal requirement to review and update its HR policies every 5 years, which has resulted in significantly outdated, and at times inaccurate, Department-wide policies. The policy issues that the OIG identified not only contribute to DOJ components' lack of knowledge of essential HR authorities and procedures, but they could weaken the Department's ability to recruit and retain highly qualified employees and to remain competitive with other federal agencies, which, as noted in last year's Top Management and Performance Challenges report, is a continuing challenge for the Department. In order to meet this challenge DOJ will need to address the existing deficiencies in its HR policies, monitor and update HR policies and guidelines as appropriate, evaluate its process for reviewing and updating policies, and prioritize efforts to consolidate all HR policies in a centralized location for components to reference and incorporate into their own policies.

Ensuring Financial Accountability of Department Contracts, Grants, and Pandemic-Related Funds

In Fiscal Year (FY) 2020, the Department of Justice (DOJ or the Department) awarded over $8.6 billion in contracts and over $5.4 billion in grants (see Figure 2). The passage of the Coronavirus Aid, Relief, and Economic Security (CARES) Act in March 2020 provided $1 billion in funding to the Department for awards to address the Coronavirus Disease 2019 (COVID-19) pandemic, most of which was to be administered by Office of Justice Programs (OJP). Oversight of its contract and grant awards to ensure financial accountability and mitigate the risks of fraud or misuse of contract and grant funds is an ongoing challenge for the Department.

Figure 2
DOJ Spending by Fiscal Year



Source: OIG analysis of data from Office of Justice Programs, Office on Violence Against Women, and Office of Community Oriented Policing Services; USASpending.gov (as of October 4, 2021).

Contracts Oversight

Effective contract oversight ensures that the Department receives products and services that fulfill its mission while detecting fraud, waste, and abuse when spending taxpayer dollars. In numerous individual contract audits over the past several years, the Office of the Inspector General (OIG) has repeatedly identified weaknesses in DOJ's management and administration of its contracts, including inadequate acquisition planning, acceptance and payment of unallowable costs, inadequate monitoring of contract performance, and inadequate training of government personnel assisting with contract administration and oversight. The Department's recurring contract oversight issues led the OIG to issue a Management Advisory Memorandum in July 2020 summarizing the deficiencies we have identified and recommending that the Department consider including contract management in its enterprise-level risk management prioritization. As the OIG's oversight findings reflect, contract oversight remains an important challenge facing the Department.

Compliance with Laws, Regulations, and Policies

As noted in last year's Top Management and Performance Challenges (TMPC) report, the Department has had difficulty complying with the Federal Acquisition Regulation (FAR) when administering and overseeing its contracts, and this issue persists. For instance, the OIG's June 2021 audit report on the Drug Enforcement Administration's (DEA) Laboratory Information Management System support contracts underscored many of the deficiencies that were highlighted in the OIG's July 2020 Management Advisory Memorandum. Among other things, the report found that the DEA did not adhere to the FAR and the DEA's internal policy, which require

Ensuring Financial Accountability of Department Contracts, Grants, and Pandemic-Related Funds

contracting officials to develop and implement a quality assurance surveillance plan along with the statement of work to monitor the contractor's performance, and that the DEA failed to consistently conduct or document the results of contractor performance evaluations. The contract also did not include required whistleblower protections clauses, which was a systemic issue the OIG notified the Department about in a February 2021 Management Advisory Memorandum concerning the Department's compliance with laws, regulations, and policies regarding whistleblower rights and protections for contract workers supporting Department programs.

Problems with contract oversight at the Federal Bureau of Investigation (FBI) was one of the main factors that resulted in the OIG finding in July 2021 that a then-FBI Special Agent in Charge and two then-FBI Assistant Special Agents in Charge had engaged in misconduct for, among other things, their roles in an unauthorized $2 million purchase of intellectual property related to a classified undercover operation. This recent misconduct finding was preceded by an audit report in September 2020, which found that the FBI did not obtain proper authorization prior to announcing a contract solicitation for subject matter expert services, and did not properly delegate contract administration responsibilities to qualified Contracting Officer's Representatives or evaluate and report the contractor's performance.

The OIG also found additional deficiencies in administration and oversight of other contracts. For example, in September 2021, the OIG issued an audit report regarding Tax Division contracts awarded for expert witness services that identified areas of non-compliance with the FAR and internal guidance. One of the findings was that trial attorneys who were expected to handle significant contracting activities were not formally designated these responsibilities, were not trained as required by the FAR, and did not display the requisite knowledge of FAR requirements to undertake certain contract procurement and oversight tasks. Similar issues were identified in an OIG audit report in September 2020 regarding the Environment and Natural Resource's Division's procurement and administration of expert witness contracts. Further, in an audit report in July 2020 regarding the U.S. Marshals Service's (USMS) contract to operate a detention facility, the OIG found that the USMS needs to improve its contract oversight procedures, particularly regarding unmet staffing levels, processing invoice deductions, contract price reduction proposals, and the use of commissary funds. As of September 2021, 5 of the 10 recommendations remain open.

These OIG findings are examples of a pattern of weakness in contract administration and oversight, including but not limited to FAR compliance. Compliance with the FAR is particularly important because it assists the Department in procuring products and services that meet the Department's needs and ensures that the Department is conducting business with integrity, fairness, and openness. Poor contract oversight undermines the Department's ability to obtain the benefits of full and open competition, which can include lower costs and higher quality products and services.

Procurement Issues at the Federal Bureau of Prisons

Procurement issues continue to challenge the Federal Bureau of Prisons (BOP). In last year's TMPC report, we noted the OIG's concerns over how the BOP procures food, including issues related to pre-award diligence, contractor performance, and quality controls. The purchase of food products that do not meet applicable standards potentially endangers the health and safety of BOP inmates and staff. Further, addressing this issue is important for BOP financial accountability in procurements, which account for a substantial portion of the BOP's budget. For example, in FY 2019, the

Ensuring Financial Accountability of Department Contracts, Grants, and Pandemic-Related Funds

Contracts Oversight

Grants Oversight

CARES Act Administration and Oversight

Food service workers at a BOP facility
Source: BOP

BOP allocated 5.7 percent or approximately $401 million of its budget to food products and food services for the roughly 180,000 inmates housed in 122 BOP institutions. These challenges with food procurement were summarized in a Management Advisory Memorandum reissued by the OIG in 2020 and were evident in a False Claims Act settlement in January 2021 that resolved allegations regarding the sale of adulterated or substandard food products to the BOP.

Issues with healthcare contract administration at the BOP also have been repeatedly identified as a challenge during OIG audits and reviews. The OIG has previously found that the BOP faces significant challenges due to inadequate policies, pre-planning, and contract management related to healthcare. Addressing issues with healthcare contract administration is particularly important for the Department and the BOP because, from 2012 through April 2021, the BOP has held comprehensive medical services contracts with approximately 20 contractors totaling approximately $1 billion. Moreover, the failure to do so appropriately could significantly impact the adequacy and quality of healthcare provided to inmates. This challenge was exemplified in an OIG investigation that found that a BOP contractor had submitted false claims to the BOP in connection with healthcare services provided by the contractor to inmates, which resulted in a False Claims Act settlement in June 2021 for $694,593. This settlement resolved allegations that the contractor had submitted inflated claims for evaluation and management services provided by several physicians at BOP's Terre Haute, Indiana, facility between January 2014 and June 2020. Further, as of September 2021, the OIG recommendation to the BOP in 2017 to require all comprehensive medical service providers to submit electronic claims has not been closed. The deficiencies with the BOP's healthcare claims data limit the ability to identify and respond to potentially fraudulent claims and, because most of the BOP's healthcare claims are processed by paper at individual institutions, billing across the BOP cannot be meaningfully analyzed.

Over the past year, the OIG has seen similar issues in the procurement of various types of other products and services provided to the BOP. For example, the OIG's data analytics investigative efforts led to the issuance of a Management Advisory Memorandum in April 2021 expressing concerns about how the BOP procures air ambulance services. The absence of uniform guidance or contract provisions concerning reimbursement for air ambulance claims has resulted in inconsistent handling of air ambulance claims across BOP institutions and the BOP in many cases has reimbursed air ambulance claims at rates far in excess of the Medicare reimbursement rates.

Similarly, in September 2020, an OIG audit report identified several deficiencies in the contracting process related to a $3.2 million contract to update fences at nine U.S. Penitentiaries. In addition to the system-wide issues discussed above in the Maintaining a Safe, Secure, and Humane Prison System section, the OIG found that the BOP did not perform an adequate price proposal analysis to determine whether the contract had a

Ensuring Financial Accountability of Department Contracts, Grants, and Pandemic-Related Funds

fair and reasonable price. As a result, the OIG estimated that the contractor received from BOP over $900,000 in additional profit because the project took significantly less time to complete than estimated for the firm-fixed-price contract.

Grants Oversight

The total dollar amount of DOJ's grant awards has increased substantially in recent years after Congress more than tripled the annual amount of Crime Victim Funds (CVF) available for the provision of victim services through grants awarded by OJP. From FY 2015 to FY 2020, Congress appropriated over $2 billion each year in additional CVF funds, and in FY 2021, Congress appropriated over $1.2 billion in CVF funds. Each of these years, Congress provided $10 million to the OIG for oversight of these CVF grants. Separately, DOJ has received additional grant funds to specifically address the COVID-19 pandemic, which we discuss below. A continuing challenge for the Department is to ensure that it has adequate controls over the management of grant funds with respect to both CVF-related grants and other types of grants.

CVF Grants to State Entities

Established by the Victims of Crime Act of 1984, the CVF collects criminal fines and penalties which is then distributed to states and territories through grants by DOJ to support victim services.[4] OJP administers the CVF by sending states and territories funding directly through the Victims of Crime Act victim assistance and compensation formula grants and awarding discretionary grants to state and local public and private entities to support national scope projects, training, and technical assistance that enhance the professional expertise of victim service providers. From FY 2015 to FY 2020, the Department issued grants from the CVF that totaled over $14 billion. In addition to 10 audit reports about specific CVF state grants in FY 2021, the OIG issued two comprehensive audits in 2017 and 2019 on OJP's management of the CVF, which found, among other things, that CVF grant recipients struggled with monitoring thousands of subrecipients. For example, in September 2021, the OIG released an audit on three grants totaling over $100 million that found, among other things, that the grantee did not complete its monitoring activities on a timely basis and performed inadequate oversight of subrecipient financial reporting and matching funds. The report also identified over $1.5 million in questioned costs. These issues demonstrate how poor financial monitoring can increase the risk that government funds will not be used in compliance with federal regulations. In meeting this challenge, the Department must remain vigilant in its instructions to and oversight of grantees to ensure taxpayer funds are expended for the intended purpose, and to advance the objectives of the grant program.

Other DOJ Grants

In addition to the approximately $1.8 billion in CVF formula grants awarded to states and territories in FY 2020, the Department awarded over $3.6 billion in other grants (see Figure 2). The OIG continues to identify significant challenges facing the Department in its oversight of these other types of grants.

One of the most pressing challenges for the Department is implementing its new grants management system. Recently, OJP, the Office of Community Oriented Policing Services, and the Office on Violence Against Women announced that award recipients must register with JustGrants, a new grant management system that replaces and integrates the functions of the previously used Grants Management System, NexGen, and the Grants

[4] 34 U.S.C. § 20101.

Ensuring Financial Accountability of Department Contracts, Grants, and Pandemic-Related Funds

Payment Request System. As the OIG explained in an issue alert in May 2021, the Department's transition to JustGrants has impacted the OIG's ability to effectively manage oversight efforts because of delays and difficulties obtaining accounts for JustGrants. Other potential problems with the transition include access to funds, which can affect an award recipient's ability to achieve program missions, goals, and objectives. For example, the OIG has observed challenges to award recipients caused by, among other things, educating and training award recipients on how to use the system and once registered, difficulties submitting required documentation (e.g., Performance Reports, Federal Financial Reports, award modification requests, and required award closeout information). The OIG has initiated an audit of OJP's contract awarded for the JustGrants system to assess its implementation, administration, and performance and compliance with the terms, conditions, laws, and regulations applicable to the contract. In the meantime, the Department must successfully complete the transition to JustGrants in order for it to be able to effectively administer its grants program.

In addition to implementing a new grant management system, the Department faces the challenge of effectively managing its large grant portfolio. In the OIG's recent oversight of non-CVF state grants, which included issuing 17 reports in FY 2021, the OIG has identified findings in areas that included a lack of adequate monitoring, poor grant financial management, and unsupported and unallowable grant expenditures. Although the Department has an effective award system in place, the consistency of these findings demonstrates that the Department continues to face the challenge of effectively managing its grant portfolio.

CARES Act Administration and Oversight

The COVID-19 pandemic has presented the Department with a variety of unexpected and unanticipated challenges, including administrating additional grant funds and contracts. The CARES Act appropriated approximately $1.007 billion to the Department, with $850 million allocated to OJP to award Coronavirus Emergency Supplemental Funding (CESF) grants for the purposes of preventing, preparing for, and responding to the pandemic. As of October 4, 2021, the Department has obligated over $930 million in CARES Act funding, which includes over $845 million in grants and over $84 million in contracts. The OIG issued two interim reports in July and November 2020 that reviewed OJP's administration of CARES Act funding, in which the OIG found that, generally, OJP had distributed CESF funding quickly and in accordance with CARES Act requirements and that oversight of CESF funds must remain a priority for OJP and the OIG, especially considering the extent to which CARES Act funding provided through the CESF overlaps with CARES Act funding provided by other federal agencies. In September 2021, the OIG issued the final audit report, finding, among other things, that OJP acted quickly to distribute CESF funding and that most recipient spending reviewed appeared allowable under the terms and conditions of the awards. However, the report noted that, as of March 31, 2021, CESF recipients reported spending or obligating only 40 percent of the total amount awarded and OJP must continue to carefully monitor CESF funds to ensure they are spent in the manner intended.

Combatting COVID-19-Related Fraud through Effective Enforcement

One of the most significant new challenges facing the Department is the need to effectively investigate and prosecute fraud and other violations of law related to the over $5 trillion in emergency pandemic spending that has been enacted since March 2020. The Pandemic Response Accountability Committee (PRAC) and the U.S. Government Accountability Office have

Ensuring Financial Accountability of Department Contracts, Grants, and Pandemic-Related Funds

Contracts Oversight

Grants Oversight

CARES Act Administration and Oversight

detailed in its reports the significant extent of fraud and misconduct that has already been uncovered in connection with pandemic-related funds. Inevitably, the extent of wrongdoing that is identified will only continue to grow as investigations and audits are conducted, and as additional funds are disbursed. Consequently, the Department will continue to face increasing demands on its personnel and resources to investigate and prosecute COVID-19-related fraud and other wrongdoing that harms the public, while continuing to meet its law enforcement demands unrelated to COVID-19.

The Department is coordinating the efforts of its law enforcement components with the PRAC and the entire Inspectors General community. The Department announced the establishment of a COVID-19 Fraud Enforcement Task Force in May 2021 to facilitate the use of all the tools available at the federal level to combat COVID-19 fraud and invited, among others, the PRAC to be a part of the task force. As of March 2021, the Department had publicly charged 474 defendants in 56 federal districts around the country with crimes based on COVID-19-related fraud schemes, as well as using civil tools to combat fraud. These cases involve fraudulent schemes to obtain over $569 million by targeting the Paycheck Protection Program, Economic Injury Disaster Loan program, and Unemployment Insurance programs. Since then, the Department has pursued many more cases related to the pandemic, including cases prosecuted by U.S. Attorneys' Offices and the Criminal Division's Fraud Section.

A further challenge for law enforcement and prosecutors is the need to address the use of Identity theft schemes to defraud pandemic response programs, as the PRAC explained in July 2021. Identity theft to obtain COVID-19-related funds victimizes the public twice: first when an individual's personal information is misused and second when funding meant to be used in response to the pandemic is diverted to bad actors. Among other actions, in July 2021, the PRAC announced the formation of a working group focused specifically on preventing and addressing identity fraud in pandemic response programs, and it is coordinating its efforts with the Department's COVID-19 Fraud Enforcement Task Force.

In order to assess the Department's response to these various challenges, the OIG is currently conducting an audit of the Criminal Division's and the Executive Office for U.S. Attorneys' management and coordination of pandemic-related fraud allegations and referrals.

Press conference announcing the DOJ's Procurement Collusion Strike Force
Source: DOJ

Another emerging area where emergency COVID-19 pandemic spending will present a challenge for the Department is combatting COVID-19-related violations of federal antitrust law in connection with contracting and procurements. In November 2019, prior to the pandemic, the Department's Antitrust Division responded to the general challenge of procurement-related collusion aggressively, announcing the establishment of a Procurement Collusion Strike Force, composed of the Antitrust Division, multiple U.S. Attorneys' Offices around the country, the FBI, and Inspectors

Ensuring Financial Accountability of Department Contracts, Grants, and Pandemic-Related Funds

Contracts Oversight

Grants Oversight

CARES Act Administration and Oversight

General for multiple federal agencies. The Procurement Collusion Strike Force is continuing to work to detect and deter antitrust crimes, including those involving COVID-19-related procurement collusion.

The OIG will continue to coordinate with the Department in the investigation and prosecution of fraud and other violations of law related to the pandemic. This will be a significant challenge for the foreseeable future and the law enforcement demands that this challenge puts on the Department will continually increase as the Department works to uncover fraud and other wrongdoing related to COVID-19.