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

Top Management and Performance Challenges Facing the Department of Justice–2023

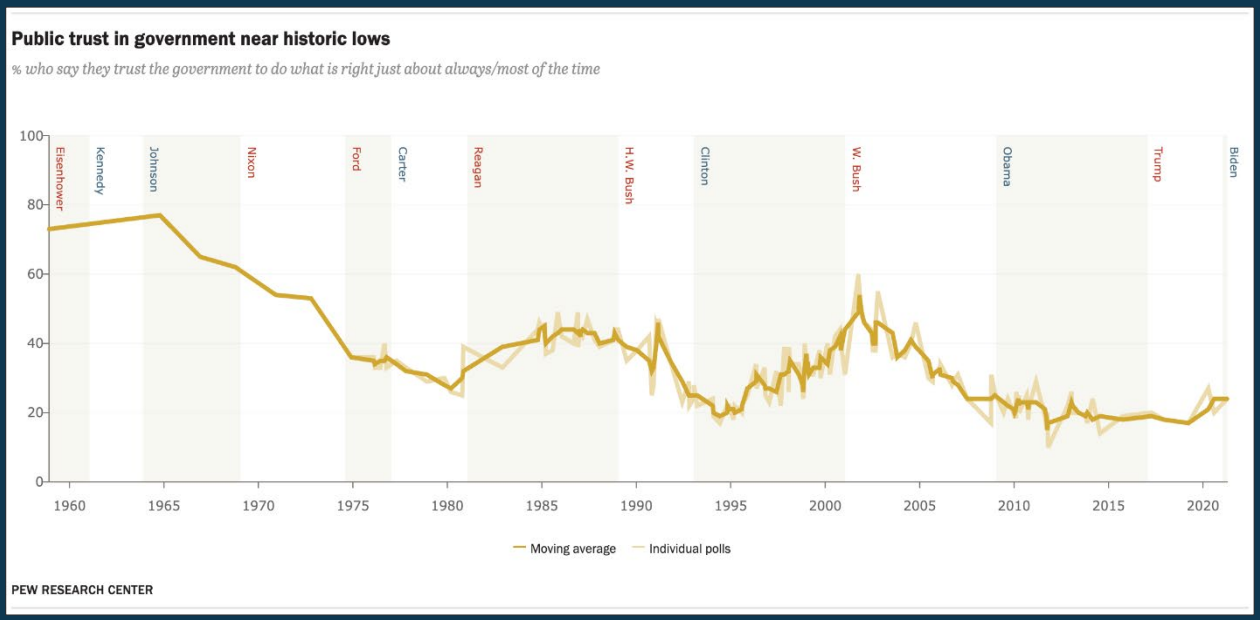
Table of Contents

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

Strengthening the public's trust in the U.S. Department of Justice (the Department or DOJ) continues to be a critically important challenge for the Department. Events over the last several years have placed the Department's objectivity and independence at the forefront of public discourse. As then Attorney General Edward H. Levi observed back in 1975, "since laws exist for the common good, they must be enforced with fairness, evenhandedness, and a proper and common concern for each individual." DOJ's preeminent challenge is to continue to strengthen public trust in the institution by ensuring that decisions and actions adhere to the Department's foundational values of independence, impartiality, and integrity. The Department can demonstrate its continued commitment to these values by ensuring that its actions are free from any actual or perceived political influence, ensuring there are appropriate measures to respond to employee misconduct, and by appropriately using sensitive investigative and law enforcement authorities entrusted to DOJ.

Ensuring that the Department is Free from Political Influence

Public trust in the federal government has approached near record lows.[1] As of June 2023, fewer than 2-in-10 Americans say they trust the government in Washington to do what is right "just about always" (1 percent) or "most of the time" (15 percent). These are among the lowest trust measures in nearly 7 decades of polling. In light of today's wide-spread lack of trust and negative views of government, a key facet of the Department's challenge of strengthening public trust is ensuring that DOJ personnel fulfill their duties without any actual or perceived political influence or partisan consideration.



Source: "Public Trust in Government: 1958-2023." Pew Research Center, Washington, D.C. (Sept. 19, 2023). https://www.pewresearch.org/politics/2023/09/19/public-trust-in-government-1958-2023/, September 23, 2023.

[1] "Public Trust in Government: 1958-2023." Pew Research Center, Washington, D.C. (Sept. 19, 2023). https://www.pewresearch.org/politics/2023/09/19/public-trust-in-government-1958-2023/, September 23, 2023.

As the Office of the Inspector General (OIG) noted in last year's Top Management and Performance Challenges report, allegations of politicization of the Department's actions are not new. One method of avoiding such allegations is strict adherence to Department policies, rules, and regulations. Failure to do so can result in actual or perceived improper influence, particularly by those in senior leadership and law enforcement positions. For example, an investigative summary the OIG released in February 2022 found that a then U.S. Attorney exercised poor judgment and engaged in conduct unbecoming of a U.S. Attorney, or any DOJ leader, and that reflected poorly on DOJ by making derogatory public remarks about a career prosecutor who added his signature to a letter signed by a number of Assistant U.S. Attorneys that was critical of a memorandum issued by then Attorney General William Barr. The OIG determined that the U.S. Attorney sought to undermine the career prosecutor's professional reputation by inappropriately suggesting that partisan political considerations motivated the prosecutor to sign the letter and implying that the prosecutors had acted unethically by signing the letter. This action was contrary to advice from a Department official and served to harm the public's perception of the Department. More recently, a May 2023 OIG report found that a then U.S. Attorney repeatedly failed to adhere to Department policies and ethics advice. The OIG concluded that the then U.S. Attorney engaged in misconduct when, among other things, she used her position as U.S. Attorney to attempt to influence the outcome of a local partisan election in Massachusetts and attended a partisan political fundraiser. The OIG concluded that the then U.S. Attorney violated government ethics regulations, Department policy, and applicable law, and failed to exercise sound judgment.[2] These examples illustrate the importance of the Department ensuring that personnel at all levels, and particularly its senior leaders, abide by governing policies, rules, and regulations that are designed to safeguard against any actual or perceived improper influence.

Protecting Against Employee Misconduct and Strengthening Oversight

The Department also faces the challenge of diminished public trust in the institution when DOJ employees fail to adhere to the basic expectations of public service. The vast majority of DOJ employees recognize that being in a position of public trust requires a commitment to uphold laws and ethical principles, as well as good judgment, honesty, and faithful fulfillment of duties. Unfortunately, prominent examples of DOJ employees who did not exemplify these core principles of public service have recently come to light. For example, in the investigation and review of the Federal Bureau of Prisons' (BOP) custody, care, and supervision of Jeffrey Epstein at the Metropolitan Correctional Center in New York, New York (MCC New York), the OIG identified numerous failures by the MCC New York staff, including the failure to perform duties, falsification of records, and multiple violations of MCC New York and BOP policies and procedure. The OIG also found significant failures in BOP personnel's job performance in the 2022 OIG report concerning the circumstances leading to the death of James "Whitey" Bulger in BOP custody. The Department's failure to adequately ensure the safety and wellbeing of two of the arguably most notorious BOP prisoners substantially weakens public trust in the federal prison system and the Department as a whole.

The BOP is not the only component facing challenges surrounding failure to adhere to the principles of public service. In August 2023, following his retirement from the Federal Bureau of Investigation (FBI), Charles McGonigal, the former chief of counterintelligence in the FBI's New York office, pleaded guilty to conspiring to violate U.S. sanctions by working on behalf of a Russian oligarch with whom U.S. entities were

[2] The Office of Special Counsel issued its report finding that the same conduct violated the Hatch Act, a statute outlining prohibited political activity for federal employees. The then U.S. Attorney resigned shortly after the OIG's and the Office of Special Counsel's reports were released.

prohibited from doing business. In September 2023, McGonigal pleaded guilty to an additional federal charge in the District of Columbia arising from allegations that he accepted $225,000 from a foreign national while still employed by the FBI and that he failed to complete the required financial disclosure form.

Incidents such as these can contribute to a lack of trust and confidence generally and undermine the perception of the Department as an institution of integrity. It is therefore critical that those who engage in such misconduct are held accountable for their wrongdoing. Unfortunately, in an OIG review released in 2021 we found that, in addition to policy, training, and recordkeeping gaps, the FBI does not regularly document substantiation decisions when employees resign or retire during the misconduct adjudication process. This practice fails to hold accountable former FBI employees who separate while under investigation and enables FBI employees to avoid a substantiation decision if they resign or retire before the FBI issues a decision in the pending misconduct matter. The FBI concurred with all of OIG's recommendations and is working to implement all the recommended corrective actions.

Another way to provide assurance to the public that former DOJ officials will be held accountable for any misconduct they commit while employed at DOJ is for Congress to confer upon the OIG the authority to subpoena witnesses for testimony in OIG investigations, audits, and reviews. While the OIG has authority to compel DOJ employees to provide testimony during OIG administrative misconduct investigations, the OIG does not have the ability to compel the testimony of former DOJ employees. Additionally, the OIG does not have the authority to compel the testimony of current or former employees of DOJ-employed contractors or DOJ grant recipients. As a result, the OIG is unable to interview former DOJ employees, or current or former employees of DOJ-employed contractors or DOJ grant recipients, about alleged misconduct by them in connection with their work for the Department or use of DOJ funds. The OIG has had numerous instances where DOJ employees or DOJ-employed contractors retire or resign simply to avoid having to answer for their alleged misconduct, which often impedes the OIG's ability to fully learn the facts in investigations, audits, and reviews in which former employees or contractors decline to be interviewed. Without this information from the OIG, DOJ components may lack the information necessary to hold wrongdoers accountable. In 2022, the Strengthening Oversight for Veterans Act of 2021 was signed into law, which authorized the Department of Veterans Affairs OIG to issue subpoenas for testimony, including from former employees. Extending this same authority to the DOJ OIG would increase public trust by enabling the OIG to fully investigate alleged wrongdoing, to hold wrongdoers accountable, and to provide a more fulsome account to DOJ leadership, Congress, and the public.

Another important aspect of strengthening public trust in DOJ is ensuring that allegations of attorney professional misconduct are handled no differently than allegations against other DOJ employees. At present, allegations of professional misconduct by DOJ attorneys are handled by the DOJ's Office of Professional Responsibility, not the OIG. Unlike the OIG, the Office of Professional Responsibility lacks statutory independence from the Attorney General and the Deputy Attorney General. As Inspector General Michael Horowitz explained in his congressional testimony, there is no principled basis for authorizing OIG oversight of DOJ law enforcement personnel, including the FBI, while excluding DOJ lawyers from the same statutorily independent oversight. The OIG has the means and expertise to handle misconduct allegations against DOJ lawyers. Providing statutorily independent oversight of DOJ attorneys would strengthen public confidence in the review of these misconduct allegations.

Ensuring Responsible Use of Investigative Authorities

U.S. Capitol

Source: Sheik/stock.adobe.com

Another continuing challenge for DOJ is to conduct national security and criminal investigations and prosecutions in a responsible manner that protects civil liberties. As then Attorney General Robert H. Jackson observed, "The prosecutor has more control over life, liberty, and reputation than any other person in America." It is therefore imperative that the Department exercise its investigative authorities in a manner that balances its investigative and prosecutorial interests against fundamental rights and freedoms. The need for this balancing is particularly acute with respect to activities protected by the First Amendment—including the right to assemble and petition the government for redress, as well as the freedom of the press. To help the Department meet this challenge, the OIG continues to work on ongoing reviews and investigations that examine the response of DOJ and its law enforcement components to public protests, including an investigation into use of force allegations involving DOJ law enforcement personnel in Portland, Oregon, in 2020; a review examining DOJ and its law enforcement components' roles and responsibilities in responding to protest activity and civil unrest in Washington, D.C., in 2020; and a review of DOJ's role and activities in preparing for and responding to the events at the U.S. Capitol on January 6, 2021.

A free and open press is protected by the First Amendment and central to the functioning of our democracy. Similarly, as Congress is a separate branch of government, the Constitution's Speech or Debate Clause was, according to the U.S. Supreme Court, "designed to assure a co-equal branch of the government-wide freedom of speech, debate, and deliberation without intimidation or threats from the Executive Branch. It thus protects Members of Congress against prosecutions that directly impinge upon or threaten the legislative process." The Department, on occasion, faces the challenge of conducting criminal investigations while protecting a free and independent press, as well as the activities of members of Congress. In 2021, Attorney General Merrick Garland issued a memorandum that prohibits DOJ attorneys from using "compulsory legal process for the purpose of obtaining information from or records of members of the news media acting within the scope of newsgathering activities," with limited exceptions. Pursuant to this memorandum, DOJ developed regulations, which were implemented in 2022. To increase accountability and transparency, the OIG is conducting a review to address concerns about the circumstances in which these authorities were used before the Department's new policy and regulations were in place. This review will examine DOJ's use of subpoenas and other legal authorities to obtain communication records of the news media and members of Congress and affiliated persons in connection with recent investigations of alleged unauthorized disclosures of information to the media by government officials.

Another critical area for strengthening public trust is the Department's use of its investigatory powers under the Foreign Intelligence Surveillance Act (FISA). Enacted in 2008, Section 702 of FISA authorizes the U.S government to conduct surveillance of foreign persons reasonably believed to be located abroad to acquire foreign intelligence information. Section 702 specifically prohibits the targeting of U.S. persons, any person located in the United States, and any foreign person located abroad for the purpose of targeting a U.S. person or person inside the United States with whom the foreign person is communicating. However, even when deployed properly, surveillance under Section 702 can result in the incidental collection of communications involving or concerning U.S. persons, which raises significant civil liberties concerns. To address these concerns, Section 702 requires specific procedures to minimize the acquisition, retention, and sharing of any information concerning U.S. persons. As discussed in the Promoting and Safeguarding National Security challenge, the current debate regarding the potential renewal of Section 702, which expires at the end of the year, reflects the tension between the competing concerns and underscores the need for responsible use of this investigative authority.

As detailed in a 2022 Foreign Intelligence Surveillance Court decision, the FBI was found to have frequently violated query standards designed to ensure responsible use of the Section 702 investigative authority. As a result, the FBI implemented measures to strengthen compliance with safeguards designed to minimize data collections involving U.S. persons. A July 2023 decision by the Foreign Intelligence Surveillance Court found that while some errors remained, the FBI's compliance with the applicable safeguards had improved. As with other facets of this challenge, continued adherence to applicable policies, rules, and regulations will help the Department continue to strengthen the public's trust in its ability to wield powerful investigative tools responsibly.

The need to use sensitive investigative authorities in an appropriate manner was also brought to light through OIG oversight, which has found significant issues with the FBI's use of certain FISA authorities. In a 2019 review that examined four FISA applications (which did not involve Section 702 authorities), the OIG found that FBI personnel fell short of the FBI procedures that require agents to document support for all factual assertions contained in FISA applications to ensure the applications are "scrupulously accurate," known as the "Woods Procedures." A 2021 OIG report reviewing the FBI's execution and compliance with the Woods Procedures found numerous instances of FBI personnel failing to ensure FISA applications were "scrupulously accurate." A 2022 audit report identified several instances of ineffective coordination between the FBI's Office of General Counsel and DOJ's National Security Division and uncertainty in the delineation of their roles that negatively impact important workflows between them. As Inspector General Horowitz noted in his April 2023 testimony before the U.S. House Appropriations Subcommittee on Crime and Federal Government Surveillance, the "overarching conclusion from this series of reports is that transparency, and effective internal and external independent oversight, are necessary to ensure that the tremendous authority held by the Department's investigators and prosecutors to surveil Americans is used in accordance with applicable laws, court orders, and the Constitution."

Priority Recommendation: FBI Policy for Supervisory Review of Woods Files

The widespread non-compliance with the Woods Procedures that we identified in our 2021 audit raised serious questions about the adequacy and execution of the FBI's supervisory review process in place at the time of the applications we reviewed. Accordingly, we recommended the FBI develop and implement policy that describes the expectations for supervisory review of Woods Files, and, as part of this policy modification, consider options for incorporating an element of independent verification of the Woods File during the FISA application process. The FBI agreed with the recommendation and is taking steps towards implementation.

The Department's mission—"to uphold the rule of law, to keep our country safe, and to protect civil rights"—undergirds many of the fundamental aspects of our country's system of government and social contract. As Attorney General Levi aptly observed, "A large part of that mission involves the reinforcement of public confidence in the administration of justice." To effectively fulfill its important mission, it is imperative that the Department continues to strengthen public trust in the institution and its ability to fairly and impartially administer justice.

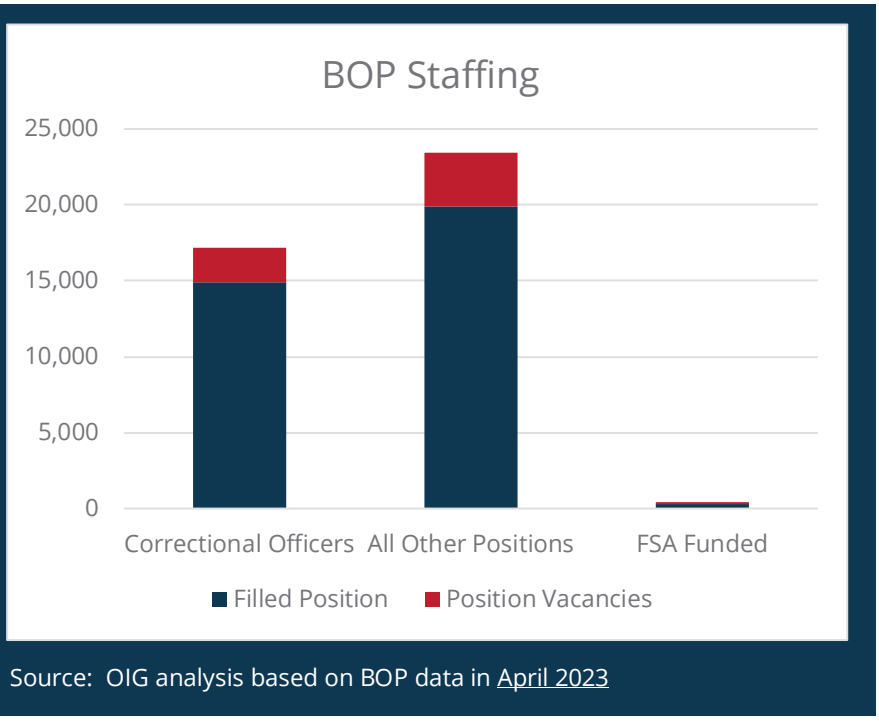
Strategic Management and Operational Challenges in the Federal Corrections System

The Federal Bureau of Prisons' (BOP) recent update to its mission, vision, and core values statements signals its renewed commitment to institutional change. In her September 2022 testimony before the Senate Judiciary Committee, newly appointed BOP Director Colette Peters announced the BOP's strategy to strengthen oversight and efficiency of its management and operations that includes plans to increase institution staffing, eradicate misconduct, improve infrastructure, upgrade camera systems, and change the BOP culture. These efforts are critical and urgently needed, but the BOP Director faces numerous obstacles to implement these proposed changes. Among the significant recurring issues the Office of the Inspector General (OIG) has identified in our oversight of the BOP are staffing and internal audits; deaths in custody; professionalism and accountability of staff; institutional safety and security, including deteriorating facilities; cost and quality of inmate healthcare, including mental health; and policy development. Adequately addressing these issues is integral to the BOP's and the Department of Justice's (the Department or DOJ) success in ensuring a safe, humane, and compassionate federal prison system.

In fiscal year (FY) 2023, the OIG launched a new inspections program and conducted separate unannounced inspections of Federal Correctional Institution (FCI) Waseca and FCI Tallahassee. The OIG identified serious facility, staffing, security, and food services issues from these inspections, and the OIG plans to continue the inspections program to assess institutional compliance with correctional policies and standards. Also in FY 2023, the OIG received additional funding from Congress to create an interdisciplinary group to address the need for additional BOP oversight. As a result, the OIG formed the BOP Interdisciplinary Team to leverage the OIG's diverse talent and collective knowledge across OIG divisions and offices to enhance and expand oversight of the BOP. The BOP Interdisciplinary Team has one overarching goal—to enhance the OIG's oversight of the BOP by increasing intra-agency collaboration and strategic work planning.

Staffing and Internal Audits

The BOP continues to face challenges in key areas, such as staffing and internal audits. Those challenges continue, and recently the U.S. Government Accountability Office (GAO), citing longstanding issues with (1) managing staff and resources and planning and (2) evaluating programs that help incarcerated people successfully return to the community, added "Strengthening Management of the Federal Prison System" to its High-Risk List to help guide DOJ's focus.



Source: OIG analysis based on BOP data in April 2023

Staffing Shortages

The OIG has highlighted the BOP's difficulties in hiring its full complement of Correctional Officers (CO) and other critical staff in previous Top Management and Performance Challenges reports in 2022, 2021, and 2020, and understaffing continues to affect BOP operations. Among the reasons this area remains a challenge is that the BOP has historically struggled to understand its actual staffing needs. The OIG's May 2023 operational issues review found that BOP Executive Staff had not adequately assessed its actual staffing needs and recommended the agency develop a reliable method of determining its needs, both at the enterprise and institution levels. In the May 2023 unannounced inspection of FCI Waseca, the OIG found that shortages of COs resulted in the regular implementation of overtime and "augmentation," the practice of assigning non-COs to CO posts to fill staffing gaps. The OIG found that these practices reduced morale and staff attentiveness thus decreasing the overall safety of the institution.

In June 2021, the BOP hired a contractor to devise a tool to assess staffing needs and challenges that the BOP faces. The BOP also created a new recruitment office with targeted campaigns and recruitment incentives. Although the BOP was able to achieve a net gain of employees in February 2023, it still faces a significant deficit of staff. In September 2023, the BOP employed 12,484 COs across its 122 institutions and had 2,393 vacancies for the same position, a 16 percent vacancy rate.

Another facet of BOP staffing shortages is the shortage of health services personnel. This is yet another long-standing challenge for the BOP, which has consistently struggled to fill such positions at its institutions. In a September 2023 review of personnel shortages in federal health care programs during the COVID-19 pandemic, the Pandemic Response Accountability Committee found that from mid-2019 through mid-2021, the BOP made progress toward addressing its shortages of health services personnel.[3] However, the overall fill rate for institution health services positions never exceeded 85 percent, and the fill rate declined from August 2021 through at least July 2022, which appears to be driven both by a decrease in hiring and an increase in resignations.

The Pandemic Response Accountability Committee report findings are consistent with a 2021 OIG survey of BOP staff perceptions of the BOP's pandemic response, which indicated that nearly one-third of BOP staff were considering leaving their jobs. Additionally, the 2022 Federal Employee Viewpoint Survey results indicated that BOP staff were dissatisfied with their job and organization and the BOP ranked last out of 432 federal subcomponents in the area of employee engagement and satisfaction. These results suggest that the BOP should consider employee engagement and retention as a core component of its strategy to address the issue of staffing shortages.

Internal Auditing

The BOP's current internal audit process, known as "program review," was created over 30 years ago. In a May 2023 OIG review, former BOP Director Michael Carvajal acknowledged that the BOP's program review process failed to reveal "major deficiencies," and that the process was unable to effectuate corrective action. The same May 2023 review found that weaknesses in the BOP's internal audit function contributed to its inability to accurately assess and improve the operations of its institutions and their programs. The OIG also noted BOP employees' fear of retaliation and their perception that the BOP's internal audit component

[3] The OIG participated in a multiagency review of health care staffing shortages resulting in a report issued by the Pandemic Response Accountability Committee.

lacked independence as contributing factors to the deficiencies in the current program. The review made several recommendations to address weaknesses in the BOP's internal audit program.

Deaths in Custody

Compliance with Policy and Procedures

The BOP recognizes the critical importance of adhering to policies, procedures, and guidelines to maintain a secure, safe, and orderly correctional environment. Yet, in the May 2023 operational issues review referenced above, the OIG cited a BOP report that reconstructed the circumstances surrounding an inmate's suicide at U.S. Penitentiary (USP) Atlanta in June 2021. The BOP had noted that between October 2019 and June 2021, five inmates died by suicide at USP Atlanta. Many of the previous psychological reconstructions had similar findings relating to staff complacency, indifference, and inattentiveness, including the "need for attention to detail, adherence to BOP policy, and regard for human life." The OIG's June 2023 report concerning the BOP's custody, care, and supervision of Jeffrey Epstein also found widespread non-compliance with BOP policies and procedures, including the failure to conduct required inmate counts, staff rounds, and cell searches. This report made eight recommendations to the BOP, including that the BOP evaluate its methods of accounting for inmate whereabouts and wellbeing. To assist the BOP with confronting this challenge, the OIG is also completing an evaluation of inmate deaths at BOP institutions from FYs 2014 through 2021 to assess the circumstances surrounding the deaths and evaluate how the BOP seeks to prevent future inmate deaths. The OIG is also investigating the circumstances surrounding the release from prison and subsequent death of Frederick Marvin Bardell, who was released from FCI Seagoville, a BOP facility in Texas, and died 9 days later in February 2021. This oversight will help the BOP address the challenge of adhering to policies and procedures designed to prevent inmate deaths in custody.

Jeffrey Epstein's jail cell after his death

Source: Office of the Chief Medical Examiner, City of New York

Single-Celling

The failure to follow sound correctional practices, along with housing inmates in a cell without a cellmate, known as "single-celling," has jeopardized institutional security and posed increased risk of inmate death in BOP custody. As detailed in the OIG report on Epstein, the placement of Epstein in single-cell confinement was contrary to express direction from BOP psychological staff and his single-cell confinement status at his time of death provided him the opportunity to die by suicide. In another OIG report on a high-profile death, the OIG found that James "Whitey" Bulger's prolonged single-celling in a Special Housing Unit prior to his transfer caused him to state that he had lost the will to live and may have affected his persistence to be assigned in general population upon his arrival to USP Hazelton.

Regrettably, single-celling deaths are not uncommon at BOP institutions. The OIG's March 2023 capstone report found that during the COVID-19 pandemic numerous facilities single-celled inmates during COVID-19 modified operations despite BOP guidance stating that facilities should avoid doing so to the greatest extent possible. The BOP reported to the OIG that seven inmates died by suicide from March 2020 through April 2021 while housed in single-cell confinement in quarantine units related to COVID-19. In a 2017 report on restrictive housing for inmates with mental illness, the OIG determined that the BOP was not limiting the length of time for inmates to spend in single-cell confinement, and that the BOP needed to track and monitor the cumulative time that all inmates spend in restrictive housing, including single-cell confinement. As of August 31, 2023, two recommendations related to single-celling from the capstone report and two recommendations related to single-celling from the restricted housing report, which included a thorough assessment of single-celling policies and increased tracking of inmates placed in single-celled confinement, remained open. The BOP's current Special Housing Unit policy, published in 2016, does not address single-celling practices.

Institutional Safety and Security

Incomplete and insufficient documentation, inconsistent application of established policies, and staffing shortages in key positions remain hurdles for the BOP in its pursuit of ensuring institutional safety. Deputy Attorney General Lisa Monaco identified these obstacles in her remarks at a BOP Warden training in April 2023. She acknowledged the "difficult job of maintaining safe custodial settings under demanding circumstances," while adding "training backlogs" and "infrastructure challenges" to the list of hurdles faced by numerous BOP institutions. When unaddressed, these obstacles compromise institutional safety and lead to significant consequences, such as the failure to prevent sexual abuse and misconduct.

Addressing Sexual Misconduct

The Department has taken steps recently to address sexual misconduct in BOP facilities. The seriousness and significance of this challenge is reflected in the widespread sexual abuse identified by the OIG in its ongoing investigation at the BOP's facility in Dublin, California, where eight employees have been criminally charged to date with sexually abusing inmates. Most prominently, in March 2023, the former Warden at FCI Dublin was sentenced to 70 months in prison after he was convicted of sexually abusive conduct against three female inmates. In response to this sentencing, Deputy Attorney General Monaco said that "this prosecution should serve as both warning and reassurance that the Department of Justice will not waver in holding accountable BOP employees and executives who abuse their authority." In an effort to address these issues, the Department launched a working group to review the Department's approach to rooting out and preventing sexual misconduct by BOP employees. A November 2022 report by the working group, among other things, outlined recommendations regarding prevention, reporting, investigation, prosecution, and employee discipline to improve the Department's response to and prevention of sexual misconduct by BOP employees. In particular, the report highlighted the need for sufficiently trained staff within the BOP's Special Investigative Services offices, which are charged with investigating staff misconduct. As an example, shortages of Special Investigative Agents have led to the frequent use of Special Investigative Services Lieutenants as initial responders to allegations of sexual misconduct by staff despite their lack of specialized sex-crime or trauma-informed training and despite the fact that these Lieutenants typically worked alongside the alleged perpetrator and reported to the leadership of the institution where the alleged perpetrator worked. The working group assessed that this, along with other factors, may deter reporting of sexual or other misconduct by staff. This shortage also leads to a significant backlog of staff misconduct cases, including those involving allegations of a sexual nature. The working group recommended that

Special Investigative Agents, who operate independently of institutional leadership, be the initial point of contact for these reports to enhance investigations and improve the BOP's response.

The OIG has also identified serious concerns with how the BOP handles allegations of administrative misconduct by BOP staff, including sexual misconduct, in investigations and disciplinary proceedings. In a Management Advisory Memorandum (MAM) issued in October 2022, the OIG notified the BOP of OIG concerns with the BOP's handling of inmate statements and testimony in staff misconduct cases. Contrary to established policy and applicable law, the BOP was not evaluating inmate testimony on a case-by-case basis. Instead, inmate testimony was largely dismissed in the absence of corroboration, which failed to adhere to the "preponderance of the evidence" standard necessary to sustain findings in administrative misconduct cases. The OIG made three recommendations to the BOP, two of which have been thoroughly addressed and considered closed.

In addition to concerns arising from BOP staff sexually abusing inmates, an OIG review identified serious concerns with inmate conduct directed toward their custodians. Inadequate recordkeeping detrimentally impacts the BOP's ability to respond to inmate-on-staff sexual assault. A February 2023 OIG report found that, when addressing inmate-on-staff sexual misconduct, the BOP had incomplete recordkeeping, particularly within the system used to track inmate violations. These records often lacked the gender of the victim, a narrative of the reported incident, and the correct prohibited act code that dictates the disciplinary action received by the offending inmate. Without complete data, the OIG concluded that the BOP could not adequately quantify the issue of inmate-on-staff sexual misconduct and thus could not implement policies to address it. This dramatically reduces institutional safety and morale of staff, leading to staff retention issues and exacerbating staffing shortages.

Security Cameras

Effective security cameras, a critical tool in maintaining safety and security in BOP institutions and assisting law enforcement to investigate and hold both inmates and staff accountable for crimes or misconduct, have been a long-standing issue for the BOP. In 2021, the OIG issued a MAM regarding needed upgrades to the BOP's security camera system that found 86 percent of the BOP's cameras (20,700 of 24,000) were utilizing old analog technology that had poor-quality video, limited coverage of areas within institutions, limited ability to zoom and search recorded video, and restricted video storage periods. The OIG recommended the BOP upgrade its video camera system to a modern, fully digital system, and that recommendation remains open as of August 31, 2023. More recent oversight work underscores that problems with the BOP's security camera system continue. For example, the OIG's unannounced inspection of FCI Waseca found shortcomings in the institution's camera system, making it difficult to monitor inmate activity and provide sufficient coverage of highly trafficked inmate areas. Additionally, as detailed in the OIG's June 2023 report, the BOP facility where inmate Jeffrey Epstein

A security camera outside a BOP facility

Source: OIG

was assigned had a history of camera problems, such as nonfunctioning cameras and recurring failures, particularly with respect to the hard drives of the camera's digital video recorder system.

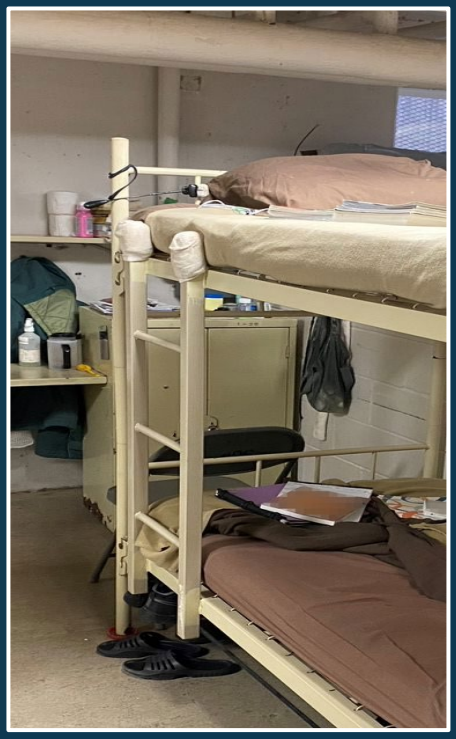
The bipartisan Prison Camera Reform Act of 2021, enacted in December 2022, shortly after congressional testimony by several BOP sexual assault victims and Inspector General Horowitz, requires the BOP to address these types of issues and ensure that its facilities have security cameras with coverage and capabilities necessary to ensure the documentation and accessibility of video evidence pertaining to misconduct, maltreatment, or criminal activity within correctional facilities. Promptly addressing the requirements in the law will assist the BOP in meeting this recurring challenge.

Priority Recommendation: BOP Strategic Plan for Transitioning to Digital Security Cameras in its Facilities

Given the consequences of inadequate, poorly functioning security cameras and the clear need BOP has in this area, in 2021, the OIG recommended that the BOP develop a comprehensive strategic plan for transitioning to a fully digital security camera system that, among other things, identifies enhancements needed to address camera functionality and coverage deficiencies, provides cost projections and the BOP appropriations account to fund the upgrades, and includes an estimated timeline for completion of the work. The BOP agreed with the recommendation and is taking steps towards implementation.

Facility Infrastructure

Another enterprise-wide challenge related to the BOP's inability to remedy operational issues connected to safety and security is its aging infrastructure. Many of the BOP's physical facilities have deteriorated to the point of literally crumbling due to a growing list of unfunded modernization and repair needs. As discussed in the May 2023 operational issues review, BOP Executive Staff commonly cited aging infrastructure as a foundational, enterprise-wide challenge that has limited the BOP's capacity to remedy operational issues. To illustrate the depth of this challenge, an OIG inspection of FCI Waseca identified serious infrastructure issues such as significant damage to several building roofs that have caused leaks throughout the institution. The OIG also found that inmates with top bunks slept in very close proximity to exposed pipes, which inmates stated regularly leaked onto their beds. After receiving a draft of this report, FCI Waseca management relocated inmates from top bunks in close proximity to pipes to other areas of the institution. Additionally, unaddressed roof maintenance caused damage to medical equipment, created food sanitation issues, and led to periodic interruption of dental care and meal services as those spaces had to be temporarily vacated due to leaks. The serious nature of these issues is not unique to FCI Waseca.



Proximity of exposed pipes to inmate beds in FCI Waseca

Source: OIG

A different May 2023 OIG report found significant infrastructure issues at several other institutions. Moreover, that audit report found that the BOP's infrastructure planning efforts were negatively impacted by two major factors: (1) a mismatch between available and needed funding, and (2) the absence of a well-defined infrastructure strategy. As of May 2022, the BOP's

estimated costs for needed, major repairs were approaching $2 billion. Yet, the BOP's budget request has been far below its estimates and resource needs. In her statement before the Senate Judiciary Committee in September 2022, Director Peters discussed prioritization projects and systems needing replacement or upgrades throughout the agency to include water and sewer distribution, electrical distribution, roof replacement, boiler replacement, fire detection, and fence replacement. Also, according to Director Peters, infrastructure attention is required to support existing systems in dire need of upgrades such as fiberoptics and communications, and fiberoptics is being installed to provide the backbone for necessary camera upgrades that are ongoing. In the May 2023 audit report, the OIG recommended the BOP develop an infrastructure strategy and establish and implement key performance indicators to validate whether the BOP is meeting its infrastructure goals.

Watch IG Horowitz Speak on the OIG's Report on the BOP's Efforts to Maintain and Construct Institutions.

(Left) Ripped ceiling at Correctional Institution Taft in California, (Right) Mold below pipes at Federal Transfer Center Oklahoma City in Oklahoma [Correctional Institution Taft was closed after it was deemed unsafe to occupy due to major infrastructure issues]

Source: OIG

Pandemic Response and Mental Health

The COVID-19 pandemic tested the BOP's ability to respond to a public health emergency that required significant operational modifications to prevent and manage the spread of COVID-19 and protect inmate and staff health and safety. It is critical that the BOP learn lessons and adapt to handle the next public health emergency, which the World Health Organization has warned is a threat.

In addition to the previously discussed March 2023 capstone report of the BOP's response to the pandemic, in May 2023, the OIG reported survey results of federal inmates' perceptions of the BOP's management of the COVID-19 pandemic. According to the results from the 25,500 inmates who responded to the survey, which was distributed to 126,000 inmates in 122 BOP institutions, inmates also reported that the medical and mental health care they received and the availability of cleaning supplies and institution sanitation worsened during this time. According to approximately 54 percent of inmates, information that the BOP

provided to inmates on how to protect themselves from COVID-19 infection was either "poor" or nonexistent.

Procurement and Financial Management

Procurement and financial management remain significant strategic management challenges within the BOP. The BOP continues to bypass the contract solicitation process through the issuance of sole-source contract actions, potentially creating significant cost risks for the BOP due to lack of competition. Although the BOP is making progress towards a comprehensive medical plan for its medical service contracts, implementation in the near term is unlikely. Additionally, the BOP continues to experience resource constraints throughout the organization that significantly impact its ability to maintain internal controls over financial management.

Contract Management and Oversight

The timely procurement and oversight of BOP contracts remains an important challenge for the BOP. In September 2022, the OIG issued a MAM highlighting concerns identified through several audits and reviews conducted since 2012 that related to the BOP's strategy for medical services contracts. Such contracts are important because medical services are a significant expense, and it is important for BOP's budgeting to optimize cost certainty in this volatile area. Although the BOP has taken corrective actions to address and close numerous OIG recommendations at the institutional level, improvements are still needed to close out many of the OIG recommendations for medical services contracts. As of August 31, 2023, 22 recommendations remain open related to medical services contracts with 1 recommendation dating as far back as 2016. Successfully executing corrective actions in response to OIG recommendations can help the BOP improve its oversight and management of inmate medical services. Additionally, the OIG completed an audit of 14 sole-source contract actions totaling $58 million that the BOP awarded to 13 contractors between FYs 2018 and 2022. The OIG identified several concerns resulting from the turnover of qualified contracting officials, using acquisition and facility personnel to "augment" its understaffed CO workforce, and lack of adequate oversight and monitoring. The OIG proposed nine recommendations to help the BOP improve its controls and activities related to its sole-source actions. The OIG has found similar issues with BOP contracting in audits of facility construction contracts, perimeter fencing contracts, and residential reentry center contracts, including inadequate acquisition planning, a sole-source award resulting in limited competition, and insufficient contract oversight and monitoring. Although the BOP has closed many of the recommendations stemming from

Front Entrance of Federal Transfer Center Oklahoma City in Oklahoma

Source: OIG

these reports, the recent sole-source contracts and medical services reports demonstrate the many challenges the BOP faces to resolve repetitive contract management and oversight deficiencies. Last, the OIG is conducting an audit of BOP contracts awarded to the American Correctional Association (ACA). The objectives of the audit are to evaluate the value the BOP receives through ACA accreditation of prison facilities. Additionally, the OIG is evaluating how the BOP uses ACA accreditation to improve BOP standards for health, safety, and security of inmates and staff.

Financial Management and Reporting

During FY 2022, the Department completed its multi-year financial management strategy to consolidate multiple financial management systems into one system by migrating the legacy core accounting system for the BOP into the Department's centralized accounting system, the Unified Financial Management System. In addition to this significant change, the BOP continued to experience ongoing challenges with workforce attrition, and—similar to the acquisition and facility personnel referenced above—BOP employees with financial management responsibility were required to augment the BOP's CO workforce duties in addition to their existing financial responsibilities.

The FY 2022 Annual Financial Statements Audit identified multiple control deficiencies related to the BOP's financial management. These included: (1) financial reporting controls not being executed by employees with sufficient training to ensure transactions were recorded in accordance with generally accepted accounting standards and financial management policy, (2) system-generated reports lacked quality information to permit management's timely and reliable execution of internal controls over financial reporting, and (3) accounting ledgers required a significant number of accounting adjustments to correct material errors that were the result of deficient internal controls over financial reporting. These control deficiencies indicated there was a reasonable possibility that a material misstatement in the financial statements would not have been prevented or detected and corrected on a timely basis, and accordingly, were reported as a material weakness in the independent auditor's report. The report included three recommendations for the BOP to improve its financial management and reporting controls.

Policy Development and Implementation

As discussed in the 2022 Top Management and Performance Challenges report, the BOP continues to face significant challenges in implementing policies required by legislation, including the First Step Act (FSA), as well as amending and updating its policies in general. The BOP has addressed concerns identified in the OIG's November 2021 MAM on the Failure to Conduct Formal Policy Negotiations on the BOP's Implementation of the FSA and Closure of OIG Recommendations by reimplementing in-person union meetings following pandemic-related restrictions and prioritizing issues pending negotiation with the national union and policies related to the FSA. However, recent GAO assessments of the BOP still show shortfalls in reaching compliance and implementing programs needed in the federal prison system. For example, in February 2023, GAO reported that the BOP had not evaluated the effectiveness of its health care reentry policies and procedures to ensure a continuity of care following an inmate's release from BOP custody. Additionally, in March 2023, GAO reported that about 45 percent of people released from federal prison are re-arrested or return within 3 years and that, despite the FSA requiring the BOP to regularly assess incarcerated people's needs and their risk of reoffending, the BOP did not have readily available, complete and accurate data regarding FSA risk and needs assessments, lacked effective monitoring efforts to assess FSA requirements and had not determined if such efforts will measure whether

risk and needs assessments are completed on time, and did not have quantifiable goals that aligned with the FSA.

In addition, as of August 31, 2023, all 5 recommendations remain open related to an OIG evaluation of the BOP's policy development process and its inability to timely update its national policies governing the actions, conduct, and conditions of employment for its nearly 35,000 staff. While the Department's FSA Annual Report in April 2023 highlights the Department's and the BOP's progress in fully implementing the FSA, there remains substantial work to do in this important area. In order for the BOP to address the numerous challenges that it faces, it will need to take action to ensure that it can effectively and timely implement revised and updated policies.

Promoting and Safeguarding National Security

FBI agent in Tampa Bay, Florida, helping with security preparations for Super Bowl LV in 2021

Source: FBI

Promoting and safeguarding national security, a core responsibility of the Department of Justice (the Department or DOJ), remains a significant challenge amid an ever-evolving threat landscape in which a range of foreign and domestic malign actors use a variety of techniques to threaten American lives, democratic institutions, critical infrastructure, economic interests, and emerging technologies. Reflecting the scope and significance of the difficult task of promoting and safeguarding national security, DOJ's fiscal year (FY) 2024 funding request includes $7.7 billion for national security programs, or over 15 percent of the Department's total FY 2024 spending request. Of this request, $32.7 million is sought to expand DOJ's counterterrorism efforts and address other national security threats. Given the overlapping and intersecting roles of the Federal Bureau of Investigation (FBI), federal partners, and other DOJ components in promoting and safeguarding national security, ensuring collaboration and cooperation across agencies and components is essential. The Department must meet this difficult challenge while also safeguarding civil liberties.

One of the new facets of this long-standing challenge is Russia's invasion of Ukraine. DOJ has sought to impose accountability on criminal networks and disrupt destabilizing national security threats arising from the invasion. The Department has responded to Russian aggression by pursuing accountability for war crimes, striking back against malign Russian cyber activity, and by limiting Russia's access to the global financial system. To this end, through its investigations and prosecutions, the Department has restrained over $500 million in assets belonging to Russian oligarchs and others who unlawfully evade U.S. economic countermeasures; charged over 30 individuals accused of sanctions evasion, export control violations, money laundering, and other crimes; and pursued arrests in over half a dozen countries. Building off this success, Attorney General Merrick Garland authorized the first-ever transfer of seized assets to the Department of State to support the rebuilding of Ukraine.

DOJ and the FBI also face the challenge of demonstrating that the FBI has implemented effective compliance tools in its use of Section 702 of the Foreign Intelligence Surveillance Act to address past compliance failures in its use of Foreign Intelligence Surveillance Act authorities, as discussed in the Strengthening Public Trust in the U.S. Department of Justice challenge. Numerous DOJ officials have identified Section 702 as a significant tool that helps DOJ achieve its national security mission. Section 702, which is scheduled to sunset at the end of this year, permits the U.S. government to acquire foreign intelligence information about

foreign persons reasonably believed to be outside the United States. The President's Intelligence Advisory Board, a group of citizens from outside the government that serves as an independent source of advice to the President on the Intelligence Community's effectiveness in meeting the nation's intelligence needs, concluded in a July 2023 report that "Section 702 is essential to generating the intelligence necessary to protect the United States from a host of threats." According to a letter to the Senate from the FBI Director, in the first half of 2023, "97 percent of the FBI's raw technical reporting on malicious cyber actors, and 92 percent of [the FBI's] reporting on emerging technologies, such as artificial intelligence, came from Section 702," demonstrating the critical need for this resource. Moreover, both the majority and minority of the Privacy and Civil Liberties Oversight Board concluded in a September 2023 report that the Section 702 surveillance program remains "highly valuable" in protecting the United States from a wide range of foreign threats, including terrorist attacks at home and abroad, cyber-attacks on U.S. critical infrastructure, and both conventional and cyber threats posed by China, Russia, Iran, and North Korea. The Board unanimously agreed that Section 702 should be reauthorized with reforms to improve protections for privacy and civil liberties, though the majority and minority differed sharply on how to address those concerns while preserving the program's value in protecting Americans' national security.

However, the compliance challenges that the FBI has faced while using this tool has highlighted the tension between protecting national security while safeguarding civil liberties. In 2022, the Foreign Intelligence Surveillance Court (FISC) found that FBI personnel had improperly queried Section 702 data in recent years, including more than 1,000 non-compliant batch queries. More recently, the FISC found that the FBI had improved its compliance. According to the FBI, reforms implemented since 2021 have substantially lowered incidents of non-compliance, resulting in a 96 percent or better compliance rate in 702 queries as of spring 2023. Also, the President's Intelligence Advisory Board July 2023 report found that DOJ has been effective in detecting non-compliance and reporting it to the FISC and Congress. Success in achieving reauthorization of what the Attorney General recently described in congressional testimony as "an indispensable tool for protecting American national security," will depend in large part on the extent to which the Department can demonstrate the effectiveness of remedial actions undertaken at the behest of the FISC, the Office of the Inspector General (OIG), the FBI Director, and Congress.

Countering Acts of Terrorism and Violent Extremism

Domestic Terrorism and Domestic Violent Extremism

Domestic violent extremists, including individual offenders and small groups, pose a significant ongoing threat to national security, with individual offenders being the primary actors in lethal domestic terrorism incidents in the United States.[4] As highlighted in the October 2022 Strategic Intelligence Assessment and Data on Domestic Terrorism, an annual report released jointly by the FBI and Department of Homeland Security (DHS), domestic violence extremists driven by a mix of ideological, socio-political, and personal grievances represent "one of the most persistent threats to the United States today." The FBI and DHS assessed that individual offenders and small groups will continue to be the primary perpetrators of domestic terrorism attacks. The report further states that these threat actors often become radicalized over

[4] According to the October 2022 Strategic Intelligence Assessment and Data on Domestic Terrorism, "[t]he FBI and DHS use the term 'domestic violent extremism' to refer to DT threats." The report defines a "domestic violent extremist" as "an individual based and operating primarily within the United States or its territories without direction or inspiration from a foreign terrorist group or other foreign power who seeks to further political or social goals, wholly or in part, through unlawful acts of force or violence dangerous to human life."

FBI agent from the Joint Terrorism Task Force

Source: FBI

the Internet, mobilize independently, and prefer easily accessible weapons, making them difficult to detect and interdict. Developing a cohesive strategy to identify these threat actors and prevent and prosecute attacks remains a significant challenge for the Department. According to the FBI Director's testimony before the House Judiciary Committee in July 2023, the FBI saw the number of FBI domestic terrorism investigations more than double since the spring of 2020. The FBI Director testified further that at the end of FY 2022, the FBI was conducting approximately 2,700 investigations within the domestic terrorism program.

In June 2023, the OIG completed an audit of the Department's strategy to address the domestic violent extremism (DVE) threat while safeguarding civil rights and civil liberties. The report included seven recommendations to help DOJ establish and maintain a cohesive approach to addressing the DVE threat, after having found that DOJ has focused efforts on investigating, prosecuting, and preventing acts of DVE, but has faced challenges in establishing a cohesive DVE strategy that would better identify lessons learned and spread awareness of available resources. While the Department has had a range of DVE-focused programs and policies in the past, some of which are ongoing, they were not consistently effective. The report found that clearer guidance across law enforcement and litigating components could promote greater consistency in classifying cases as DVE and in coordinating DVE-related cases.

The same OIG audit highlighted the need for effective collaboration across more than 15 DOJ components in combating domestic terrorism, including the FBI; Bureau of Alcohol, Tobacco, Firearms and Explosives; Federal Bureau of Prisons (BOP); Criminal Division; National Security Division (NSD), Drug Enforcement Administration; and U.S. Marshals Service. The National Strategy for Countering Domestic Terrorism, released by the White House in June 2021, likewise promotes coordination and collaboration among the federal government and its state, local, tribal, territorial, and private sector partners on combating domestic terrorism. Differing communications processes and definitions of key terms challenge the FBI's ability to effectively collaborate with partners to address national security threats. According to a report issued by the U.S. Government Accountability Office in February 2023, the FBI and DHS have collaboration agreements in place; however, the effectiveness of their collaboration has not been consistently assessed. Analyzing and implementing U.S. Government Accountability Office and OIG findings and recommendations could help the Department better respond to the difficulties posed by the sprawling and ever evolving domestic terrorism threat.

FBI Hostage Rescue Team in Quantico, Virginia

Source: FBI

Given the importance of inter- and intra-agency collaboration and information sharing in safeguarding national security, the OIG is also conducting a review of the role and activity of DOJ and its components in preparing for and responding to the events at the U.S. Capitol on January 6, 2021. The review is examining what information was available to the Department and its components in advance of January 6; the extent to which such information was shared by the Department and its components with the U.S. Capitol Police and other federal, state, and local agencies; and the role of DOJ personnel in responding to the events at the U.S. Capitol on January 6. The review is also assessing DOJ protocols, policies, or procedures to identify any weaknesses that adversely affected the ability of the Department or its components to effectively prepare for, and respond to, the events at the Capitol.

U.S. Capitol building after January 6, 2021

Source: CRAIG/stock.adobe.com

International Terrorism

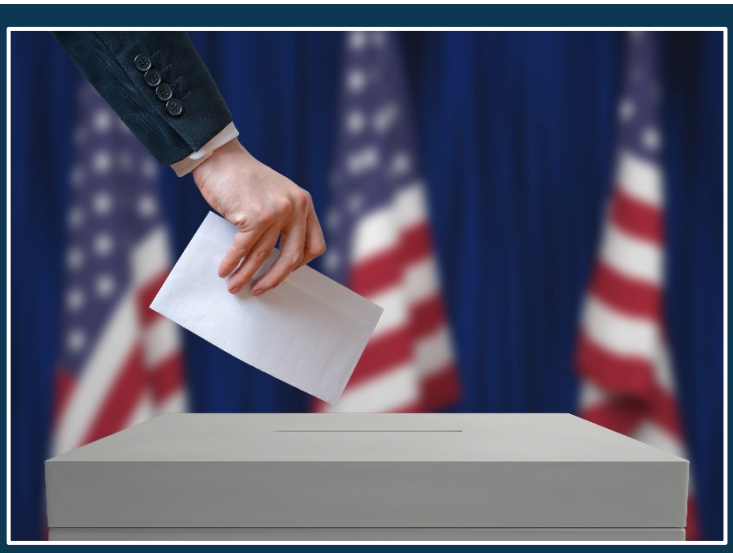
While domestic terrorism presents a significant threat to U.S. interests, international terrorism remains a longstanding and consistent challenge for the Department. The Intelligence Community continues to assess that ideologies espoused by foreign terrorist organizations and the transnational racially and ethnically motivated violent extremist (RMVE) movement pose a significant threat to U.S. persons, facilities, and interests. For example, Homegrown Violent Extremists (HVEs) continue to be inspired by Islamic State ideology and propaganda. Al-Qa'ida maintains its commitment to attacking U.S. interests, though the threat is more pronounced in the regions where Al-Qa'ida affiliates operate. Hezbollah may also seek to target the United States. Transnational RMVEs often call for attacks in the United States, and some domestic RMVE attacks have been inspired in part by transnational RMVE narratives and attacks overseas.

Previous OIG audits have provided insight into gaps in DOJ's counterterrorism efforts and recommendations for closing those gaps to effectively address the international terrorism threat. In March 2020, the OIG issued a report on the FBI's efforts to identify HVEs through counterterrorism assessments. The OIG determined that the FBI had taken insufficient steps to address the weaknesses the FBI had identified in its assessment process. As of July 2023, the OIG's recommendation that the FBI examine current field office initiatives to revisit subjects of closed assessments and investigations to determine whether all FBI field offices should undertake similar initiatives, remains open. This recommendation will help ensure consistent procedures across field offices for identifying HVEs in compliance with law and policy. In addition, a September 2022 OIG audit found several instances of ineffective coordination between the FBI's Office of General Counsel and the NSD, ambiguity in the delineation of their roles, and inconsistent interpretations by the FBI's Office of General Counsel and the NSD of key legal principles, exemplifying the need for coordination across components. As of August 31, 2023, two of the audit's five recommendations remain open. These concern coordination with the NSD and better delineating and distributing authorities to

improve oversight of the FBI's national security activities and to increase efficiency. In addition, the BOP is working to implement the remaining open recommendations from a 2020 audit report that found gaps in the BOP's monitoring of terrorist inmate communications.

U.S. Election Security and Countering Foreign Influence of U.S. Elections

The U.S. electoral process is the foundation of our democratic system of government. Promoting and safeguarding the integrity of U.S. elections and holding accountable those who seek to obstruct the orderly and lawful transfer of power as a result of elections are critical challenges for the Department. Additionally, it remains an increasing priority to ensure that all qualified voters can cast their ballots and have their votes counted, free from discrimination, intimidation, or fraud in the election process. Recognizing this challenge, DOJ's FY 2024 budget request includes $8 million to enforce federal law related to voting, including expanding the Civil Rights Division's ability to address language-access obligations, rebuild enforcement capacity, and address violations of the National Voter Registration Act.



DOJ has a role in promoting and safeguarding the integrity of U.S. elections

Source: Vchalup/stock.adobe.com

Election workers at all levels of government, whether elected, appointed, or volunteers, must be permitted to do their jobs free from threats and intimidation. The Department's interagency Election Threats Task Force, launched in 2021, partners with and supports U.S. Attorneys' Offices and FBI field offices to investigate and prosecute criminal threats; train federal, state, and local law enforcement; and engage in extensive outreach with election officials to gain greater insight into the nature of the threats they face. In the 2 years the task force has been in operation, the Department has had success investigating and prosecuting individuals who have committed election crimes, leading to multiple guilty pleas this year in Arizona, Georgia, Florida, Michigan, and elsewhere.

The FBI also remains concerned about foreign malign influence operations—which include subversive, undeclared, coercive, and criminal actions used by foreign governments in their attempts to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine confidence in our democratic institutions and processes. Therefore, the Department is active in prosecuting state agents for espionage, conducting investigations to thwart hacking campaigns, addressing through operational activity efforts to manipulate public discourse in the United States, and expanding the Foreign Influence Task Force's Russian-focused scope to include malign foreign operations of the People's Republic of China, Iran, and other global adversaries. The OIG continues to conduct a review of the

Department's efforts to coordinate the sharing of information related to foreign malign influence directed at U.S. elections. This review is examining coordination between the FBI and other components, as well as between DOJ and non-DOJ entities, and the associated challenges.

Countering Foreign Espionage

As the Attorney General noted in his March 2023 testimony, "[the People's Republic of China], Russia, Iran, and North Korea are becoming more aggressive and more capable in their malign activity than ever before." Effectively protecting confidential human sources, witnesses, operations, investigations, and its own personnel requires that the Department meet the challenge posed by the increased foreign espionage threat.

One way the Department addresses this challenge is through the FBI's undercover operations, which allows it to detect, prevent, and prosecute threats and acts related to counterintelligence, counterterrorism, cyber, and other areas. In December 2022, the OIG released a report that found several areas in which the FBI's national security undercover operations can be improved, including the under-utilization of and training provided to Certified Undercover Employees, the speed at which certain sensitive undercover operations are approved, and the tracking of short-term undercover activities that are not part of a full, authorized operation. The report made 10 recommendations to improve safety and how the FBI manages its national security undercover operations program, such as improving the tracking of undercover activities and establishing qualifications for undercover coordinators and a comprehensive training plan for undercover employees. DOJ concurred with all of the recommendations and as of August 31, 2023, continued to work on implementing them.

Safeguarding Sensitive Assets and Classified Information and Protecting Whistleblowers

Protecting sensitive assets, infrastructure, classified information, supply chains, and key technologies critical to U.S. national security and economic prosperity remain challenges for the Department. As discussed in the Department's strategic plan, 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 DOJ resources or capabilities. While insider threats and unauthorized disclosures present a serious challenge, DOJ 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 that govern the release of classified or unclassified information. DOJ managers and other leaders who encourage their employees to raise concerns promote a critical dual purpose: (1) this incentivizes DOJ personnel to report those concerns internally, rather than seeking an unauthorized outlet, such as the media, to report their concerns, and (2) when employees report internally, it provides DOJ management with an opportunity to assess and address the issue before it becomes a major problem. While DOJ employees are always protected for providing information to the OIG, the OIG also encourages all DOJ managers and leaders to familiarize themselves with whistleblower rights and responsibilities, and to discuss these rights with their employees to foster an environment that encourages lawful, internal disclosures, and thereby, discourages unlawful disclosures to unauthorized recipients.

Cybersecurity and Emerging Technology

Cybersecurity is a critical priority in view of our society's existential reliance on information technology systems for, among other things, data storage and processing, communications, and commercial transactions. The multifaceted challenge presented in the cybersecurity arena involves protecting sensitive information and systems from unauthorized access, disruption, and theft. With the increasing sophistication of cyber criminals, cybercrime poses a significant challenge to the U.S. Department of Justice (the Department or DOJ) and the nation and has led to financial losses and privacy breaches. Moreover, the rapid advancement of emerging technologies, such as artificial intelligence (AI) and new operational technologies, introduce vulnerabilities and complexities that require the Department to be agile and proactive in adapting its cybersecurity strategy to keep pace with technological changes. Enhancing cybersecurity, combatting cybercrime and cyber threats, along with adopting advanced and emerging technologies are significant challenges facing the Department.

Enhancing Cybersecurity

Cybersecurity is a risk management process—not an end state—that works to ensure information technology systems, data, and devices are protected from breaches and disruption. The Department has a leading federal role in the government's cybersecurity strategy, as outlined in the March 2023 White House National Cybersecurity Strategy. In addition, the Department relies on technology systems for its mission and operations. The Department's fiscal year (FY) 2022–2024 Information Technology Strategic Plan outlines goals to elevate cybersecurity to strengthen its security posture against complex cybersecurity attacks, improve and fortify internal remote access for the mobile workforce, and streamline identity and access management. Further, the Department's 2022 Comprehensive Cyber Review identified several areas where the Department could improve its practices in order to increase its cybersecurity related to electronic communications, mobile device security, and contractor cybersecurity requirements. As risks to systems increase with advancing technology, it is critical that the Department is vigilant in maintaining and modifying as necessary its comprehensive cybersecurity strategy as an effective risk-management program.

DOJ has a leading federal role in the government's cybersecurity strategy

Source: NicoElNino/stock.adobe.com

Cyber Supply Chain Threats

The Department, like many federal agencies, relies on commercially-available technology solutions to fulfill its mission and support its critical functions. Globalization, outsourcing, and digitization have resulted in complex, diverse, and extensive information technology supply chains that leave DOJ with less control and visibility into its supply ecosystems. Cyber supply chain threats pose a significant risk as bad actors may exploit vulnerabilities in the supply chain to gain unauthorized access to government systems by targeting

suppliers, vendors, or partners. Such attacks can lead to devastating consequences, including data breaches, supply chain disruptions, intellectual property theft, and potential harm to end-users. To help the Department better confront the challenge presented by cyber supply chain risks, the Office of the Inspector General (OIG) released an audit report in July 2022 that found, among other things, that the Justice Management Division (JMD) lacked the personnel resources needed for an effective cyber supply chain risk management (C-SCRM) program, as well as widespread non-compliance with C-SCRM requirements, outdated C-SCRM guidance, inadequate threat assessments, and insufficient mitigation and monitoring actions. The OIG also found that Federal Bureau of Investigation (FBI) procurement officials often improperly bypassed the FBI's C-SCRM program due, in part, to misunderstanding or unawareness of C-SCRM requirements. As of August 31, 2023, 15 of the 17 recommendations made by the OIG to assist the Department in managing cyber supply chain risks remained open. Addressing the open recommendations will help JMD and the FBI enhance risk mitigation and monitoring of the risk across all DOJ components.

National Institute of Standards and Technology (NIST) Critical Success Factor: Supply Chain Information Sharing

NIST states that an effective information-sharing process helps to ensure enterprises can gain access to information critical to understanding and mitigating cybersecurity risk in the supply chain, and also share relevant information to others that may benefit from or require awareness of these risks. NIST's key practices for establishing and participating in supply chain risk information sharing relationships include:

- establishing information-sharing goals and objectives, specifying the scope of information sharing, and establishing information-sharing rules;
- using secure, automated workflows to publish, consume, analyze, and act upon supply chain risk information;
- participating in information-sharing efforts; and,
- proactively establishing supply chain risk information-sharing agreements.

Safeguarding Data and Information Systems

An important part of cybersecurity is ensuring the data and information systems are secured and protected. The Department has a responsibility to appropriately safeguard its data and information systems. The importance of data security was illustrated in February 2023, when the U.S. Marshals Service suffered a major security breach. Hackers broke into and stole data from a computer system that included law enforcement sensitive information such as information related to "ongoing investigations, employee personal data, and internal processes" as well as "sensitive files, including information about investigative targets." The Department responded to this incident by conducting an inventory of all components' systems with the goal of ensuring that all were properly approved and in compliance or could be brought into compliance with DOJ requirements. DOJ's response is ongoing.

Pursuant to the Federal Information Security Modernization Act (FISMA), the OIG regularly tests the effectiveness of Department components' information security policies, procedures, and practices and the security of their systems. These audits identify weaknesses in controls that may need to be strengthened to ensure systems and data are adequately protected. In FY 2022, the OIG assessed many different component-specific information systems, specifically, those belonging to the Environment and Natural Resources Division, Office of Justice Programs, Federal Bureau of Prisons, Civil Division, FBI, and JMD. A majority of the FY 2022 FISMA audits led to at least one recommendation designed to strengthen component-specific information systems. As a member of the law enforcement and intelligence community, and as custodian of highly sensitive law enforcement and national security information, it is imperative the Department ensure its systems are secure. An aspect of doing so is giving high priority to

addressing the FISMA audit recommendations for improving the deficiencies the OIG identified in the systems we assessed. In a November 2022 memorandum to all DOJ component heads, the Deputy Attorney General emphasized the importance of the FISMA process as an opportunity to strengthen the Department's defenses against cyberattacks, intrusions, and data breaches. She directed that components whose systems were audited by the OIG promptly address the OIG's recommendations, and that components not reviewed by the OIG consider their vulnerabilities in view of the OIG's findings in the audited components. This appropriate step by Department leadership recognizes the importance of addressing system vulnerabilities. As of September 2023, there are currently 47 open FISMA recommendations from all FISMA audits conducted across the Department, indicating that work remains to be done.

Combatting Cybercrime and Cyber Threats

Cyber threats can adversely impact national security and the economy. As a law enforcement agency, the Department has an integral role in protecting the nation against these threats and leading the response to cyber incidents. Combatting cybercrime and cyber threats to the nation's security remains among the Department's highest priorities as part of its mission to ensure public safety against threats foreign and domestic and to provide federal leadership in preventing and controlling crime. Some of the challenges the Department currently faces include threats from ransomware, the difficulties of federal and global coordination for combatting cybercrime, and the mobility and high demand for highly trained cyber staff.

Ransomware

Ransomware continues to be one of the leading cyber-based threats to national security. Cybercriminals deploy ransomware and digital extortion attacks against federal agencies and U.S. businesses and organizations. In May 2023, the Department indicted a Russian national and resident for using three different ransomware variants to attack numerous victims throughout the United States, including law enforcement agencies and other sectors. In another recent example, the FBI covertly disrupted the Hive ransomware variant in January 2023, captured its decryption keys, and offered the keys to victims worldwide, which prevented payment of $130 million in ransom demands. To combat ransomware attacks, the Department created the Ransomware and Digital Extortion Task Force to strategically target the ransomware criminal ecosystem as a whole and collaborate with domestic and foreign government agencies as well as private sector partners to combat this significant criminal threat. The OIG has an ongoing audit to assess the Department's strategy to combat ransomware threats, and response to and coordination on ransomware attacks against public and private entities, which will assist the Department in addressing this significant challenge.

Federal and Global Coordination for Combatting Cybercrime

In a July 2022 Comprehensive Cyber Review, the Department recognized that successfully combatting cyber and cyber-enabled crime cannot be accomplished by any single government agency or private firm. In its national lead role, it is key that the Department coordinates with other government agencies and on a global level. In response to the U.S. Government Accountability Office's (GAO) September 2022 report on federal agency collaboration in preventing and responding to ransomware, the Department is developing a working group to share ransomware incident-related information and facilitate interagency coordination. Further, as highlighted in another GAO report issued in March 2023, DOJ also provides direct assistance to fighting cybercrime and works with foreign nations to help combat these technology-driven crimes. Global

collaboration activities include information sharing with foreign partners on current threats and providing cyber training to foreign law enforcement. The report cited a lack of dedicated resources, difficulties in retaining highly trained staff, and inconsistent definitions of "cybercrime." Continuing to build collaboration across the nation and increasing capacity globally will aid DOJ in combatting increasingly widespread and complex cybercrime.

Enhancement of Cyber Workforce

The Department relies on a host of dedicated and talented personnel to respond to, investigate, and disrupt cyber threats—including attorneys, Special Agents, Intelligence Analysts, computer scientists, data analysts, forensic technicians, and others. The Department identified difficulties in retaining cyber-related personnel due to compensation disparities between the Department and the private sector, as well as with other government departments and agencies. According to the Department's July 2022 Comprehensive Cyber Review, the Department of Homeland Security and the Department of Defense have taken steps toward addressing similar problems by creating new types of federal civil service positions for their cyber-specialized employees. These and other federal entities have also utilized cyber-specific pay incentives to attract candidates. With the rapid proliferation of cyber threats, including ransomware and other malicious attacks, it is imperative that these roles are filled with highly qualified personnel who understand both the technology and the potential applications. In confronting this challenge generally, the Department must be among the forefront of government employers taking available steps to be competitive for the most capable staff, for whom there is great demand, in the highly mobile marketplace for their skills.

Advanced and Emerging Technologies

Advanced and emerging technologies present both opportunities and challenges for the Department. AI and technologies such as forensic analysis systems have increased in capability and complexity for law enforcement and other uses in the Department. Technologies can advance operational needs, but also require workforce and infrastructure readiness, ongoing adaptation, and attention to critical privacy and national security issues. This evolving landscape presents challenges for the Department to proactively strategize and respond to emerging risks so as to not be outpaced by technological change.

The evolving technology landscape presents challenges for the Department

Source: Putilov_denis/stock.adobe.com

Strategic Planning and Adoption of Emerging Technologies

The Department's Comprehensive Cyber Review identified a lack of coordination in emerging technology efforts across components and cited potential risks in duplication of effort. Additionally, the review included

recommendations for a standing interdisciplinary body, established principles of use, and upskilling a cyber workforce in order to reduce barriers to adoption of emerging technologies.

One technology frequently discussed across government and society at-large is AI, which can be used for a wide range of applications from completing an individual task to simulating broad human behavior.[5] In response to a requirement in Executive Order 13960 Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, the Department reported 15 AI use cases to a federal annual inventory in June 2023, an increase from 4 AI use cases submitted a year prior in June 2022. The Department has been using AI techniques such as machine learning to classify and detect anomalies in drug samples, topic modeling and clustering to consolidate records review, machine translations, and other algorithms to manage information such as tips to law enforcement, multimedia data, and case documents. However, the most recent publicly issued strategy on AI from the Department—which outlines an AI adoption and coordination strategy with DOJ component responsibilities—is from 2020. The use and prevalence of AI is growing at a rapid pace and is currently available mainstream in various forms. As GAO reported in May 2023, federal agencies cannot afford to be reactive to the risks and consequences of AI. Further, as noted in GAO's September 2022 report, data privacy risk management is another significant topic to address in this area.

Key AI issue areas include system-level governance, data security, and privacy. Considering GAO's guidance on responsible federal use of AI and data privacy will assist the Department in strategizing and coordinating the adoption and governance of AI.

Responding to Changing Operational Technology

Technologies that advance or impact investigations and law enforcement operations for the Department are particularly vital. These can include new communication technologies, end-to-end encryption of data, and facial recognition technology. Specifically, FBI Director Christopher Wray's May 2023 congressional testimony cited a key concern in keeping pace with operational technologies that are becoming increasingly important to combatting criminal and terrorist threats. Technologies cited by Director Wray were forensic advancements and body worn cameras. Recently, the OIG initiated an audit of the FBI's efforts to respond and adapt to changing technologies in the environments where it operates. The audit objectives are to determine the sufficiency and effectiveness of the actions the FBI is taking to respond to changing technological environments and the training the FBI provides to its personnel to increase the workforce's adaptability to those changes. After initiating the audit, in December 2022, the OIG issued a classified Management Advisory Memorandum (MAM) to the FBI when the OIG's initial audit work revealed that certain aspects of the FBI's efforts to respond to changing operational technologies were inadequate and required better communication and coordination, and prompt corrective action. The classified MAM included two recommendations to help ensure that the FBI employs a more robust and effective strategy to address the risks posed by changing operational technologies and that its workforce is better positioned to identify and adapt to those risks. The FBI concurred with both recommendations and stated that it has already begun taking necessary corrective actions. Addressing the OIG's recommendations in the MAM, and any recommendations that result from the current audit, will help the Department as it responds to changing operational technologies.

[5] GAO, "Artificial Intelligence," https://www.gao.gov/artificial-intelligence (accessed September 20, 2023).

Pursuing the Department's Law Enforcement Mission While Protecting Civil Rights and Civil Liberties

Like other law enforcement agencies, the U.S. Department of Justice (the Department or DOJ) faces an ongoing need to prioritize transparency and accountability, particularly relating to use of force and safeguarding civil rights and civil liberties. At the same time, the Department must ensure that sufficient strategy and resources are dedicated to pursuing long-standing, large-scale challenges, such as violent crime and opioid and narcotic interdiction; emerging priorities, such as pandemic-related relief fraud; and the protection of vulnerable populations, such as children.

Police officer badge

Source: Fergregory/stock.adobe.com

Protecting Civil Rights and Ensuring Accountability

The Department continues to face the important challenge of carrying out its law enforcement operations while fulfilling its duty to protect civil rights and civil liberties. For example, as the Department continues to reform and modernize its own law enforcement practices and policies, it faces the challenge of ensuring adequate oversight of and accountability for its investigative tools and programs so that they align with the full spectrum of the Department's duties and legal obligations.

Use of Force

The Department serves as a lead entity for the May 2022 Executive Order (EO) 14074, Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety. In the aftermath of the most recent racially charged events involving law enforcement, this EO has the stated goal of placing "federal policing on the path to becoming the gold standard of effectiveness and accountability" while imposing requirements to modernize federal policing and improve safety, accountability, and public trust. The Department continues to take action including issuing guidance banning the use of chokeholds and carotid restraints, restricting the use of "no knock" warrants, and updating DOJ's use-of-force policy with officers' affirmative duty to intervene and render medical aid as well as receive de-escalation training. Moreover, coinciding with the issuance of an Office of the Inspector General (OIG) audit report

U.S. Marshals Service (USMS) agents conducting a law enforcement operation in Baltimore, Maryland

Source: USMS

in June 2021, the Deputy Attorney General directed all DOJ law enforcement components to establish and implement a body worn camera (BWC) program.

Police BWC

Source: Skyward Kick Prod/stock.adobe.com

In September 2023, the OIG issued an audit of DOJ's use-of-force policies within its law enforcement and corrections components. We found that DOJ law enforcement and corrections components made substantial progress towards updating their policies and training to align with DOJ's updated requirements. However, we also identified certain policy gaps related to use-of-force in custodial situations, and some components' use-of-force policies and practices were inconsistent in their application to task force officers and contractors. In addition, DOJ has not identified a mechanism to help ensure components' training programs are consistent, appropriate, or complete. We made six recommendations to minimize potential risks associated with use-of-force tactics. While these steps are important to DOJ's objective of modeling accountability in law enforcement practices, DOJ should consider further leveraging its leadership role in the law enforcement community to create incentives for state and local entities to: (1) promote community engagement, (2) remedy racial disparities in policing where they exist, and (3) improve public trust in law enforcement. The persistent challenge for DOJ is to lead the nation's law enforcement community to eliminate race-based differences in operational activities and improve community perception of equitable treatment. In May 2023, as a part of the EO, the Department issued guidance to its law enforcement components regarding the use of race, ethnicity, gender, national origin, religion, sexual orientation, gender identity, and disability in the performance of federal law enforcement and intelligence activities to ensure that those agencies gather and depend on information that is reliable and trustworthy while promoting unbiased conduct during federal law enforcement and intelligence activities. Among other things, as part of DOJ grants to state and local law enforcement agencies, such entities could be required to demonstrate commitment to safe and accountable policing practices, such as those described in the EO and implementation of a BWC program.

Oversight and Accountability

Internal and external oversight and accountability are other mechanisms for the Department to protect civil rights and civil liberties. DOJ's fiscal years (FY) 2022–2026 Strategic Plan identifies goals of establishing a culture of transparency and accountability and promoting trust between communities and law enforcement. In 2023, the Department's Civil Rights Division concluded investigations of the Minneapolis Police Department, City of Minneapolis, Louisville Metro Police Department, and Louisville/Jefferson County Metro Government, and found that each entity engaged in a pattern or practice of conduct that violates the U.S. Constitution and federal law, including use of excessive force. Each entity entered into an agreement in principle to negotiate consent decrees with the Department to resolve the investigative findings. Such remedial actions resulting from Department investigations are one way in which the Department can meet its above goals.

Watch IG Horowitz Speak on the OIG's Report on DOJ's Policy on Body Worn Cameras.

To further help the Department achieve its transparency and accountability goals, the OIG continues reviewing DOJ policies and practices protecting civil rights and liberties. In advance of the OIG's BWC report, the Deputy Attorney General, with notice of the OIG's concerns, directed that all DOJ law enforcement components establish and implement policies to use BWCs, which enhance transparency and accountability in law enforcement.

Currently, the OIG has an ongoing audit of the DOJ's Electronic Recording of Statements Policy (Justice Manual 9–13.001) governing electronic recording of custodial statements by the Department's law enforcement components. The preliminary objective is to assess component-level policies and procedures implemented to effectuate the policy. The intent of the policy was to ensure an objective account of interactions with people held in federal custody, thus providing federal law enforcement officials indisputable accounts of statements and documenting that detained individuals are afforded their constitutionally protected rights. The OIG review of component-level policies and procedures will help ensure that these Department law enforcement components are exercising their authority properly and are accountable for their treatment of individuals in their custody in connection with those individuals' statements. In addition, in August 2023, the OIG initiated an audit of the Department's Special Deputation Program to determine if the USMS, which oversees the program, established adequate policies, procedures, and controls. In September 2023, the OIG issued an audit report that assessed how the Office of Justice Programs solicits, receives, and reviews complaints of unlawful discrimination by recipients of DOJ grants and cooperative agreements, including civil rights violation allegations against law enforcement and correctional components receiving DOJ funds. This audit found that the Department can promote greater awareness of the civil rights complaint process to ensure that the public is knowledgeable about civil rights protections, and Department components responsible for responding to complaints can better work together to more efficiently address pressing civil rights violations and concerns.

Targeting Violent Crime: Gun Violence

Combatting violent crime is a longstanding and significant priority for DOJ. Ensuring the Department is prepared to meet commitments set out in its FYs 2022–2026 Strategic Plan, Comprehensive Strategy for Reducing Violent Crime, and strategy update, particularly as they relate to the issue of gun violence, will be an ongoing challenge. A Federal Bureau of Investigation (FBI) report issued in April 2023 revealed that U.S. active shooter incidents increased by 66.7 percent in 2022 compared to 2018. The FBI's report found that in 2022, there were a total of 50 active shooter incidents in 25 states and the District of Columbia, involving 61 firearms.

A handgun seized by the USMS

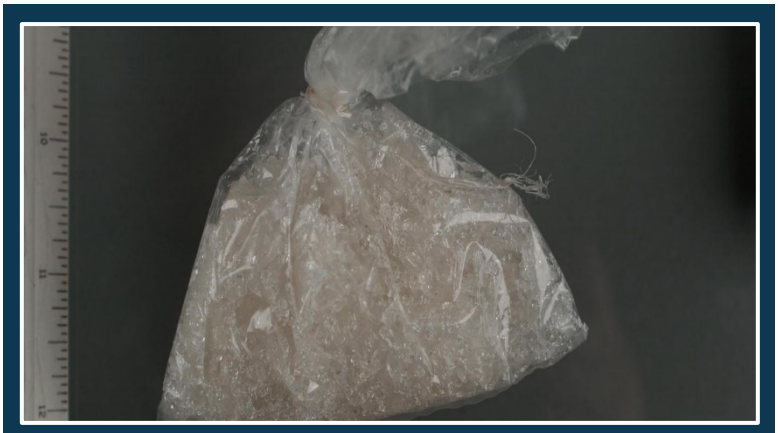
Source: USMS

The Department's FYs 2022–2026 strategic plan outlines several strategies to address gun violence and other violent crime, as well as specific goals to reduce gun-related violent crime by September 30, 2023. These include increasing the percentage of urgent firearm trace requests completed within 48 hours, the percentage of firearms cases that target traffickers or other large-scale enterprises, and the number of inspections of federal firearms licensees (FFL). Additionally, this year the Department has awarded over $238 million to states, territories, and the District of Columbia under the Byrne State Crisis Intervention Program. These awards will be used to fund extreme risk protection order programs, also known as "red flag laws," which keep guns out of the hands of those who pose a threat to themselves or others.

As the federal agency responsible for regulating federal firearms licenses, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) conducts inspections to ensure FFLs operate in compliance with laws and regulations and in a manner that protects public safety. These inspections review an FFL's inventory and transaction records to, among other things, detect and prevent the illegal diversion of firearms and reduce the possibility of firearms being obtained by prohibited persons. During our past audit work the OIG identified significant challenges facing ATF in performing its regulatory responsibilities due to significant resource constraints, as well as steps that ATF can take to improve its FFL inspections program. Most recently, in April 2023, the OIG released an audit report that found ATF had taken measures to address previous OIG findings related to the effectiveness of ATF's oversight of FFLs, but that additional improvements were necessary. The OIG made 13 recommendations to ATF to strengthen its compliance inspection activities and its oversight of FFLs. Specifically, the OIG recommended that ATF develop modern tools, such as employing predictive analytics, and that ATF revise its policies and procedures concerning the examination of inspection results to effectively identify high-risk FFLs. Implementing these recommendations could help enable ATF to not only increase the number of FFL inspections as described in DOJ's strategic plan, but also increase the efficacy of those inspections.

Opioids and Narcotics Interdiction

Drug trafficking and interdiction continue to be pressing challenges for the Department. According to Centers for Disease Control and Prevention data, after 2 years of sharp increases, overdose deaths leveled off in 2022. However, there were still approximately 110,000 recorded overdose deaths in 2022, 48 percent higher than pre-pandemic totals. According to this same data, opioids and synthetic opioids make up the vast majority of reported overdoses, and fentanyl is the leading cause of death for Americans between the ages of 18 and 45.



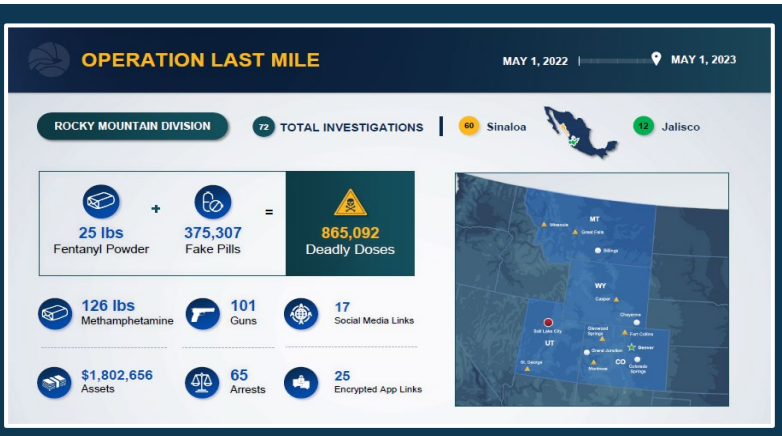
Methamphetamine seized by the Drug Enforcement Administration (DEA)

Source: DEA

Violent, international criminal organizations and cartels have become increasingly prevalent in opioid and fentanyl trafficking. U.S. Customs and Border Protection reports that the amount of fentanyl seized at the border has risen significantly from FY 2021 to FY 2023. In April 2023, the Attorney General announced

charges against the Sinaloa Cartel for running the "largest, most violent, and most prolific fentanyl trafficking operation in the world." The Department also brought charges in June and October 2023 against China-based companies and their employees with crimes related to fentanyl production, distribution, and sales resulting from precursor chemicals.

The Department's ongoing efforts to detect and seize dangerous drugs include its Joint Criminal Opioid and Darknet Enforcement team, along with international partners, conducting a coordinated international effort spanning three continents to disrupt fentanyl and opioid trafficking on the darknet or dark web. To counter the global criminal networks most responsible for the influx of fentanyl into the country, the Sinaloa and Jalisco Cartels, the DEA has created counterthreat teams for each cartel to map, analyze, and produce targeting information for the cartels' operations. Additionally, in June 2023, the Department closed an OIG audit report that contained recommendations to the DEA to improve the strategic management and oversight of DEA-supported foreign law enforcement units. In particular, the OIG coordinated with the DEA to close recommendations involving the initiation and verification of host nation agreements for DEA-supported foreign law enforcement units, as well as the bilateral use of its judicial wire intercept program.



DEA Operation Last Mile targeted operatives, associates, and distributors affiliated with the Sinaloa and Jalisco Cartels

Source: DEA

Besides large, complex operations with international elements, Department entities must also partner and work closely with state and local law enforcement to detect and disrupt opioid and fentanyl trafficking. The DEA worked with state and local law enforcement partners nationwide to seize approximately 44 million fentanyl pills and 6,500 pounds of fentanyl powder. The operation specifically targeted those responsible for the last mile of drug distribution, both in the community and on social media. A recent OIG audit report found that Department components can better coordinate and leverage resources to work with federal, state, local, and tribal law enforcement agencies and prosecutors to combat the opioid crisis. The OIG made four recommendations to assist the Department in better coordinating efforts to address this crisis. As of August 31, 2023, three recommendations remain open. The OIG is in the process of conducting an audit of the Bureau of Justice Assistance Comprehensive Opioid, Stimulant, and Substance Abuse Program to determine, among other things, if the Bureau of Justice Assistance effectively coordinated and collaborated with Comprehensive Opioid, Stimulant, and Substance Abuse Program partners and stakeholders.

Countering the Intensifying Threat of Child Exploitation

The Department recognizes child exploitation as "one of the most reprehensible and destructive offenses confronting our nation today." In 2006, DOJ launched Project Safe Childhood, which was originally aimed at utilizing federal, state, and local resources to pursue technology-facilitated sexual exploitation of children,

and was expanded in 2011 to include all federal crimes based on sexual exploitation of a minor. In 2023, DOJ released its third National Strategy for Child Exploitation Prevention and Interdiction, which described child exploitation as "an ongoing public health crisis" that "requires a whole-of-society strategic response."

The evolution of the scale and type of online threats to children poses a particular challenge for DOJ. Reports of suspected child sexual exploitation have grown substantially with the number of reported images, videos, and other content, increasing from approximately 45.8 million files in 2018 to 88.4 million files in 2022.[6] According to a December 2022 report issued by the U.S. Government Accountability Office, multiple factors are driving this growth in online threats, including use of end-to-end encryption and the ability of offenders to share content and network in dark-web communities.

As noted in past oversight work, the Department's ability to vigorously pursue child exploitation offenses will be aided by clear internal policies and guidance. A 2021 OIG report identified concerns with the FBI's efforts to notify victims of child sexual abuse material, and a 2022 Management Advisory Memorandum noted the FBI's lack of a policy governing the transmission of child sexual abuse material over email. In 2021, the OIG released a report that found multiple violations of FBI policies and concluded that FBI employees failed to treat allegations against Former USA Gymnastics Physician Lawrence Gerard Nassar with the "utmost seriousness and urgency that they deserved and required." The OIG is conducting an ongoing audit of the FBI's compliance with laws, regulations, and policies related to its handling of tips of hands-on sex offenses against children and mandatory reporting of suspected child abuse. Finally, the U.S. Government Accountability Office has recommended the Department regularly update its National Strategy for Child Exploitation Prevention and Interdiction and take other steps to improve its capacity to pursue child exploitation offenses, as required by the PROTECT Our Children Act of 2008.

Priority Recommendation: FBI Coordination with State and Local Authorities on Allegations of Crimes Against Children

In response to the FBI's mishandling of the sexual abuse allegations against Larry Nassar, in 2021, we recommended that the FBI reassess its policies to more precisely describe when FBI employees are required to promptly contact and coordinate with state and local law enforcement and social service agencies after receiving allegations of crimes against children that potentially fall under state jurisdiction, even when the allegations also potentially fall within the FBI's jurisdiction. Given the direct impact of the FBI's failure on the victims, resulting reduction of public trust in law enforcement, and the potential to mitigate similar situations in the future, the OIG believes implementation of this recommendation should be a DOJ priority. The FBI agreed with the recommendation and is taking steps towards implementation.

The Department's Ongoing Efforts to Combat Pandemic-Related Fraud

As noted in the 2022 Top Management and Performance Challenges report, the distribution of an unprecedented amount of federal disaster response funds in a relatively short time frame without sufficient controls resulted in a significant increase in fraudulent activities. More than 3 years after the passage of the first emergency pandemic relief bill, the Department

[6] Noting a "distinct rise in the enticement of children, especially minor girls, for sexual imagery" during the COVID-19 pandemic, along with the emergence of "sextortion," in which children are threatened with the release of explicit content unless they provide more content or compensate the extorter. President and CEO, National Center for Missing & Exploited Children, Prepared Remarks, before the U.S. Senate Committee on the Judiciary, concerning "Protecting Our Children Online" (Feb. 14, 2023), www.judiciary.senate.gov/imo/media/doc/2023-02-14%20-%20Testimony%20-%20DeLaune.pdf.

continues to deal with the effects of massive amounts of fraud associated with the over $5 trillion in pandemic-related funding. The Pandemic Response Accountability Committee and its member Inspectors General have estimated that the amount of fraud associated with pandemic relief programs exceeds over $100 billion. The ongoing challenge for the Department is ensuring that it has, and can dedicate, sufficient investigative and prosecutive resources to hold accountable those engaged in this pernicious fraud. DOJ's FYs 2022–2026 strategic plan notes that reports of financial victimization via fraud, especially Internet-enabled fraud, reached all-time highs in 2020. As of August 2023, the Department's COVID-19 Fraud Enforcement Task Force's coordinated efforts resulted in criminal charges against more than 3,000 defendants and the seizure of more than $1.4 billion in relief funds.

Programs meant to help individuals and small businesses, including the Payment Protection Program (PPP), Economic Injury Disaster Loans, and Unemployment Insurance (UI) benefits were particularly exploited, as these programs were launched with few, if any, controls to check if the applicant was legitimate and qualified for aid. Passing time has revealed both the ease with which fraud occurred and the prevalence of fraudsters. Bad actors participated in far-reaching and multi-jurisdictional schemes to magnify their ill-gotten gains. In addition to domestic criminals, including violent street gangs and prison inmates committing UI fraud, international organized criminal groups have also targeted these funds by using stolen identities to file for UI benefits. Examples include an individual charged with participating in a scheme to submit more than 100 applications to seven financial institutions and fraudulently obtain over $13 million in PPP loans, an individual convicted of collecting personally identifiable information of numerous individuals from the dark web and using the identities to file at least 180 fraudulent UI claims in two separate states, and a foreign national convicted of recruiting others to a scheme that sought over $3 million in PPP loans.

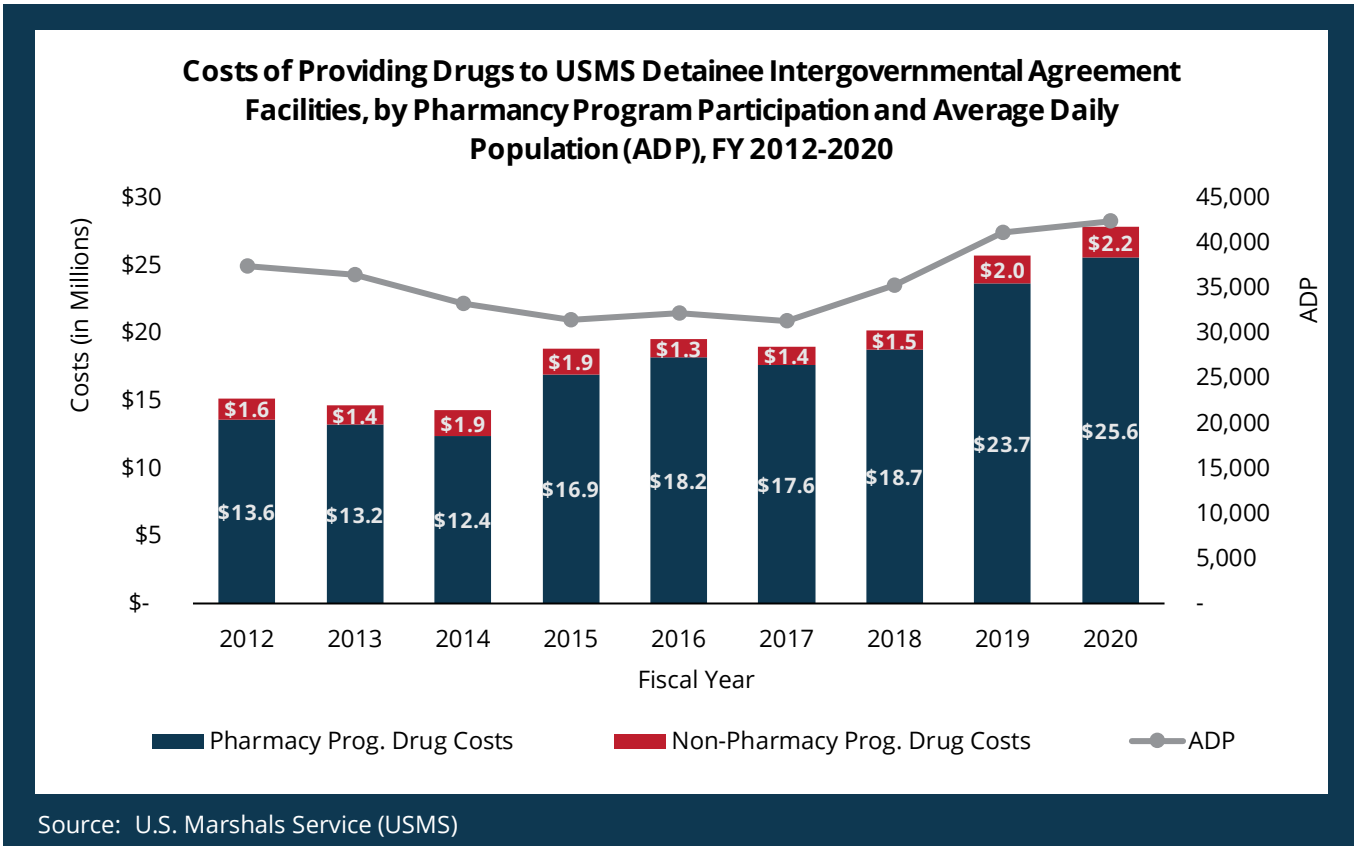
Recognizing the ongoing challenge, the Department launched its COVID-19 Fraud Enforcement Task Force in 2021 to coordinate DOJ's nationwide prosecution efforts. Additionally, Congress extended the statute of limitations for all forms of PPP loan fraud and all COVID Economic Injury Disaster Loans fraud to 10 years to allow investigators the time necessary to fully pursue those who defrauded these two programs. The Department will need to continue to coordinate with its more than 30 partner agencies as it pursues and recovers the massive amounts of defrauded relief funds. A previous OIG audit issued in 2022 found that Department components can better coordinate and utilize their finite resources to more effectively track, refer, and prosecute pandemic-related fraud matters. While all associated recommendations in the report were closed in July 2023, the Department must continue to identify and utilize all possible efficiencies considering the large amounts of fraudulently obtained funds that continue to be discovered.

Improving the Management and Oversight of U.S. Department of Justice Contracts and Grants

In fiscal year (FY) 2022, the U.S. Department of Justice (the Department or DOJ) awarded over $8.6 billion in contracts and $4 billion in grants. The management and oversight of contracts and grants remains a challenge for the Department. In particular, areas of concern include planning and oversight throughout the procurement lifecycle and grant financial management practices.

Contract Management

To ensure responsible use of public funds, it is incumbent upon the Department to conduct robust acquisition planning and contract oversight and strengthen its contract planning, monitoring, and compliance with laws and regulations.



Source: U.S. Marshals Service (USMS)

Procurement and Acquisition Planning

Proper procurement and acquisition planning promotes full and open competition and helps ensure DOJ meets its procurement needs in the most cost-effective and timely manner. Opportunities exist for DOJ to improve compliance with acquisition planning requirements to receive a fair and reasonable price for goods and services. The Office of the Inspector General (OIG) has repeatedly identified deficiencies in procurement planning that have resulted in DOJ components entering into contracts with significant cost uncertainty. For example, a December 2022 OIG report that examined the USMS's pharmaceutical drug costs and procurement process found that there was no cost control for drugs purchased by non-pharmacy

program facilities for which the USMS was separately invoiced. Consequently, the OIG found that the USMS was at risk of paying unnecessarily high prices for drugs purchased by those facilities. Further, in a September 2022 report on the Federal Bureau of Prisons' (BOP) procurements awarded for medical services provided to Residential Reentry Management Branch inmates, the OIG found that the BOP's inadequate acquisition planning and market research resulted in award pricing that was not cost effective or supported by price justifications.

Examples of poor acquisition planning by Department components has not been limited to medical services contracts. In a July 2023 report on the Office of Justice Programs' (OJP) procurement for JustGrants, a new grants management system, the OIG found that inadequate coordination and ineffective planning early in the process significantly affected OJP's ability to deliver JustGrants as intended. Compliance with Federal Acquisition Regulation (FAR) requirements also ensures that procurement and acquisition planning result in contracts that maximize taxpayer dollars. However, the OIG's JustGrants report also found that a lack of clarity in the original solicitation and blanket purchase agreement resulted in significant cost increases after task orders were issued and implemented. In addition, an August 2023 report on the Community Relations Service's contracting activities, the OIG identified several areas of non-compliance with FAR and DOJ requirements, including a lack of written acquisition plans or market research. In a November 2022 report on the Executive Office for Immigration Review's (EOIR) procurement of an electronic case management system, the OIG found that EOIR and Justice Management Division acquisition planning documents lacked multiple FAR and DOJ requirements. Insufficient evaluation of requirements and stakeholder input may result in the selection of systems that do not adequately meet the agency's needs.

Proper acquisition planning also ensures that appropriate consideration is given to the costs and trade-offs involved in a procurement. In a March 2023 report on the USMS's implementation of Executive Order 14006, which prohibits DOJ from renewing contracts with privately operated detention facilities, the OIG reviewed concerns related to the decision to replace the USMS's expiring contract with a private contractor via an agreement with a local government entity, which then contracted with the same contractor and continued to house the detainees at the same facility. The new agreement increased the USMS's costs and provided the USMS with less direct oversight of the facility. The OIG found, among other things, that not all costs and benefits of the conversion had been disclosed to responsible officials, which raised concerns about whether the decision was fully informed.

Exterior fence at BOP Correctional Institution Taft in California [Correctional Institution Taft was closed after it was deemed unsafe to occupy due to major infrastructure issues]

Source: OIG

Administration and Oversight

More than 3 years after the OIG issued a Management Advisory Memorandum (MAM) that notified DOJ of systemic issues related to contract management, DOJ components continue to face challenges in contract

administration and oversight, which involve actions performed after a contract has been awarded to determine how well the contracting parties execute the requirements of the awarded contract. By improving contract management, DOJ can mitigate risks, reduce costs, minimize delays, and strengthen the negotiation of contracts awarded.

DOJ components continue to face challenges in contract administration and oversight

Source: NicoElNino/stock.adobe.com

Several recent audits of Department contracts illustrate the issues and the challenges DOJ needs to address. For example, in an August 2023 report on OJP's contract awarded for the Office for Victims of Crime training and technical assistance center, the OIG found that OJP did not have a quality assurance plan in place until the final month of the 5-year procurement, limiting the assurance that consistent monitoring occurred throughout the procurement. In addition, in the OIG's July 2023 report related to OJP's procurement for JustGrants, the OIG found that OJP did not adequately establish a quality assurance plan that would allow OJP contracting officials to effectively monitor progress, nor did OJP ensure that duties delegated to its contracting officer's representative were fully executed and documented. The OIG identified similar issues in the EOIR case management system report, which found that government and contract personnel in oversight roles did not receive timely training, were not certified, and were not always properly designated. Ensuring timely training, certification, and designation will help to strengthen components' ability to provide effective contract oversight and administration.

Moreover, the OIG has repeatedly found that some DOJ components do not ensure that contractor performance evaluations are entered into the Contract Performance Assessment Reporting System, which is an important component of performance monitoring. The FAR requires that this information be entered at least annually during the contract evaluation periods. As detailed in audit reports issued in September and November 2022 and September 2023, the OIG found that for contracts issued by the BOP and EOIR, necessary performance information was either not added to the Contract Performance Assessment Reporting System or the information was late, incomplete, or did not cover the evaluation periods. Non-compliance places DOJ at greater risk of relying on the services of suboptimal contractors, which can result in delays, subpar products or services, or wasteful spending.

Additionally, ensuring all contracts contain mandatory whistleblower protections is critical in helping the federal government remain efficient and accountable, and to ensure appropriate stewardship of taxpayer dollars, as we discussed in the 2022 Top Management and Performance Challenges report and detailed in a 2021 MAM. Unfortunately, the OIG continues to find, as recently as August 2023, that Department contracts omit statutorily mandated clauses regarding whistleblower rights and protections for contractor employees, which show that the problem persists.

Contracts for medical services entered into by the BOP and the USMS present a particularly high risk for the Department because of the significant and rising costs for such services and related products, such as pharmaceuticals. As noted above, the OIG has found deficiencies in acquisition planning that have resulted in these DOJ components entering into contracts with significant cost uncertainty. A September 2022 MAM highlighted concerns stemming from multiple reviews of such contracts conducted by the OIG. In addition to inadequate planning for its medical services contracts, the OIG identified other issues with BOP's contracting strategy, including weak contract oversight and limited competition for contract awards. It is essential for the Department to develop and implement a comprehensive strategy that ensures transparent, efficient, and cost-effective procurement and acquisition planning processes.

Grants Oversight

The Department continues to face challenges in effectively managing its portfolio of grants, as evidenced by the OIG's numerous audits of grant recipients awarded millions of dollars, resulting in many recommendations to enhance DOJ's administration and monitoring of awards, help grant recipients better achieve compliance, and effectively implement grant recipients' programs. During the past year, OIG grant audits continued to find that grant recipients need to improve their programmatic oversight, as well as their oversight of subrecipients of grant funding. With over $4 billion in grant funds awarded in FY 2022 alone, the oversight of grants, which has also been identified in nearly every year's Top Management and Performance Challenges report, remains a challenge for the Department. This challenge is further complicated by the need to prevent and detect fraudulent activity by recipients of grant funding, which unfortunately the OIG continues to find on occasion. For example, in January 2023, the former Chief Executive Officer of an anti-poverty nonprofit pleaded guilty to embezzling and misusing more than $600,000 in grant funds. This past fiscal year, OIG grant fraud investigations resulted in grant recipients being sentenced for grant fraud in Iowa, Nebraska, and Puerto Rico. The OIG will continue to work with the Department to combat this type of fraud and ensure responsible stewardship of federal funds.

Grants Management System

The Department's plan for JustGrants was to deploy a single system that would allow applicants, grantees, and DOJ grantmaking components to move seamlessly through the full grants management lifecycle. However, in addition to the contracting issues identified above, the audit report showed that despite years of planning, the new system had a significant negative impact on users (both the federal employees and recipients). In response to a survey of users conducted in April 2022, 91 percent of users stated they experienced technical difficulties with JustGrants. Ultimately, OJP was forced to provide multiple extensions to financial, programmatic, and other reporting that compromised DOJ's ability to provide effective oversight of the billions of dollars in awards it makes each year. While JustGrants is operational and functioning for deployed features, in FY 2023, OJP continues to resolve technical issues, build out additional system functionality, and provide training opportunities to JustGrants users.

Programmatic Oversight

The OIG's oversight activities ensure recipients use grant funds in a manner consistent with their intended purpose and in compliance with regulatory and statutory requirements. The OIG's ongoing grant oversight touches on some of the most critical issues facing the United States today. For example, the OIG is currently auditing the Office on Violence Against Women's efforts to administer grant funding during the COVID-19 pandemic. The oversight is critically important, especially as we continue to assess and understand the

impact of COVID-19 on intimate partner violence. The OIG is also auditing OJP's Comprehensive Opioid, Stimulant, and Substance Abuse Program. As opioid-related deaths remain elevated, our efforts to determine if OJP is effectively managing the program and coordinating with stakeholders will provide valuable information to the Department. Finally, in April 2023, the OIG initiated an audit of the Office of Community Oriented Policing Services (COPS Office) hiring program, which provides funding directly to law enforcement agencies to increase their community policing capacity and crime prevention efforts. The audit will determine if the COPS Office made recent awards in accordance with applicable guidance and assess the COPS Office's efforts to monitor those awards. In addition to providing important grant oversight, this work can also provide valuable insight into how DOJ collects and uses data to ensure the most vulnerable communities across the country receive the assistance they need.

Oversight of Grant Recipients

During the past year, OIG grant audits continued to find that OJP needs to improve its oversight to ensure grant recipients improve their financial management, programmatic and financial reporting, and monitoring of subrecipients. Specifically, in FY 2023 the OIG identified nearly $1.1 million in questioned costs, suggesting that grant recipients need to improve their administration and management of award funds. The OIG also found deficiencies related to grant recipients' accomplishment of program performance goals in audit reports issued in December 2022 and February and March 2023. Further, in reports issued in November and December 2022, the OIG found that audited recipients had budget management and reporting deficiencies. The OIG will continue its oversight of grant-funded programs to help ensure effective grant management, oversight, and responsible use of federal funds.

OJP needs to improve its oversight of grant funds

Source: Song_about_summer/stock.adobe.com

Crime Victims Fund

The OIG plays an important role in detecting and deterring waste, fraud, and abuse in programs designed to improve how crime victims receive the support and assistance they need. To support the important oversight of Crime Victims Fund (CVF) programs, Congress has transferred $10 million annually to the OIG since FY 2015 for dedicated oversight of CVF programs and activities. With these funds, the OIG has audited approximately 21 percent ($4.2 billion) of the total CVF funds awarded ($20.7 billion) and released over 85 audit reports resulting in nearly 600 recommendations since FY 2015. CVF audit reports issued in June 2023 found that Kansas and Alabama state administering agencies—which administer the CVF funds by subawarding these funds to local organizations that provide services to victims—lack adequate policies and procedures to ensure accurate reporting of performance or financial activities. Additionally, in May 2023

the OIG again found that a grant recipient submitted inaccurate certification reports, which serve as the basis for determining the amount of certain future CVF awards, possibly resulting in awards that were hundreds of thousands of dollars over and under the appropriate amount. These issues, which have been discussed in previous Top Management and Performance Challenges reports, unfortunately persist.

Due to the OIG's concerns with the monitoring performed by state administering agencies, the OIG has begun auditing CVF funds subawarded to organizations that provide services to victims. Recent work in this area indicates that many subrecipients of grant funds struggle with financial management and limiting their use of federal funds for allowable purposes. For example, in audit reports issued in May and September 2023, the OIG identified that the CVF subawards may have been used for unallowed purposes, such as an educational program for individuals who are not crime victims. Further, in another report issued in May and that same report issued in September 2023, the OIG identified issues with subrecipients inappropriately disclosing victim information. While OJP does not have a direct role in monitoring subrecipients, DOJ must be attentive in its oversight of CVF state-level grant recipients to provide reasonable assurance that these grant funds are used as intended and in accordance with applicable laws.

The OIG oversees CVF funds

Source: NicoElNino/stock.adobe.com

Effectively Managing Human Capital

The U.S. Department of Justice (the Department or DOJ) faces multiple, interrelated human capital challenges affecting recruitment, retention, and the work environment. In the Office of Personnel Management's (OPM) 2022 Federal Employee Viewpoint Survey (FEVS), nearly 30 percent of DOJ employees reported that they were considering leaving the agency due to telework or remote work options. Moreover, according to the Partnership for Public Service's DOJ performance dashboard, by 2025, 31 percent of DOJ employees and 73 percent of DOJ Senior Executive Service (SES) managers will be eligible for retirement. This data highlights the potential human capital crisis DOJ could face if it is not sufficiently attentive to the evolving market factors that drive employee recruitment and retention. DOJ should ensure that it is using all tools at its disposal, including various hiring authorities and innovative recruitment programs, to maintain a competitive posture in the market for top quality, diverse employees across all of its components and disciplines. Related issues are the critical importance of employee recruitment, safeguarding merit systems principles in hiring, and maintaining a workplace free of harassment and discrimination.

Workplace

As DOJ continues to execute and evolve its return to the office plans, it will be crucial to plan and implement strategies that meet the needs of remote, hybrid, and in-person employees while continuing to accomplish DOJ's mission. It will also be critical for the Department to be open to policy revisions to address potentially adverse reaction to implementation of its plans. Other related challenges are managing for top performance, retaining top talent, and addressing diversity and equity concerns.

Return to Workplace

As discussed in the Office of Management and Budget's (OMB) April 2023 memorandum regarding evolving agency work environments, revised return-to-workplace plans require thoughtful consideration to ensure a smooth transition for federal employees while making sure decisions are based on how to achieve each agency's mission most effectively. In the wake of DOJ's September 2023 memorandum announcing that, with certain exceptions including for remote work, employees will be required to work in person at least 6 days per pay period starting in January 2024, the Department will face the challenge of retaining talented workers. In 2022, even before DOJ announced this new policy, 26 percent of DOJ FEVS respondents—approximately 7 percent more than the federal government-wide average—disagreed when asked if their agency's workplace re-entry arrangements were fair in accounting for employees' diverse needs and situations. A July 2023 letter from the DOJ Gender Equality Network expressed concern about the impact that increased, inflexible in-person work requirements would have on employees with caregiving responsibilities and those

Employees returning to work

Source: Jacob Lund/stock.adobe.com

with disabilities. The Department and its components face the challenge of fairly implementing the new in-person work policy's exceptions and attempting to ensure that employees have a "meaningful" in-person work experience, as the September 2023 DOJ memo and the April 2023 OMB memo require.

Another challenge will be carefully monitoring the effect of the new in-person work policy on employee retention, productivity, and morale. By leveraging workforce data, DOJ can determine whether its return-to-workplace plan succeeded in meeting organizational goals or must evolve further. DOJ can also monitor steps other federal agencies are taking with respect to workplace flexibilities, so DOJ can remain competitive and learn what has worked at other agencies.

Managing for Top Performance

Managing for top performance in the work environment that is more virtual than before the pandemic is another significant challenge across the federal government, including at DOJ. The Department scored approximately 10 percent below the government-wide averages on two 2022 FEVS questions related to management: (1) only 41.5 percent of DOJ respondents feel their management makes effective changes to address the challenges faced, and (2) only 33.1 percent feel their management involves them in decisions that affect their work. As OPM notes, setting clear goals, providing regular feedback, and maintaining open lines of communication are essential components of remote management. OPM also recommends that supervisors work to recognize strong performance by teleworkers, reinforcing a sense of motivation and accomplishment. Ensuring equal opportunities for advancement also remains a top priority. According to 2022 FEVS data, DOJ scored approximately 6 percent worse than the government-wide averages on two questions related to employee opportunities: (1) only 58.7 percent of DOJ respondents feel they have similar access to advancement opportunities as others in their work unit, and (2) only 63.4 percent feel their supervisor provides opportunities fairly to all employees.

Retaining Top Talent and a Workforce that Reflects Our Nation

Law enforcement agents participating in a tactical training exercise

Source: Federal Bureau of Investigation (FBI)

A significant challenge facing DOJ is retaining highly skilled individuals due to competition from the private sector and other federal agencies, its more limited work flexibilities than others, and the federal salary structure. These challenges can hinder the Department's ability to maintain a qualified and diverse workforce. As it seeks to retain its most productive and valued employees in the highly competitive employment market for the most qualified personnel, the Department will need to be mindful of its employees' interest in and support for enhanced workplace flexibilities. The 2022 FEVS indicated that 22.6 percent of DOJ employees (nearly 4 percent more than the government-wide average), excluding those considering retirement, were considering leaving the agency due to their current telework or remote work options. With a handful of exceptions, the 2022 FEVS data indicates that DOJ is underperforming, compared to other federal agencies, with respect to human capital issues. Failing to keep pace with the competition will hurt the

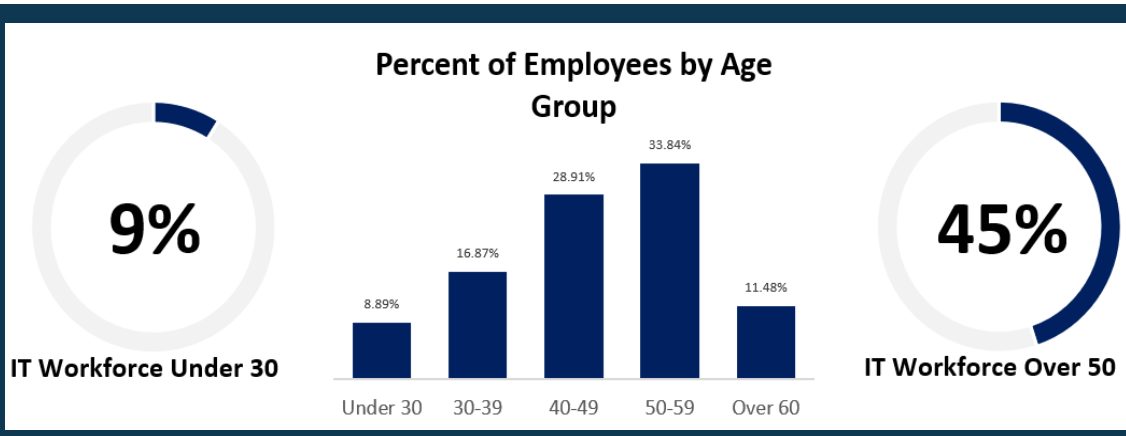
Department in its employee retention as well as employee hiring efforts, potentially resulting in DOJ sacrificing what has traditionally been its greatest strength—the talented staff dedicated to DOJ's mission across components.

The OIG's oversight work can help the Department address concerns about equity in the workplace, which in turn will help maintain a diverse and inclusive workforce. The OIG's ongoing review of racial equity in DOJ's law enforcement components is examining components' demographics, retention, attrition, promotions, and awards, and is surveying staff perceptions related to equity. The OIG's December 2022 evaluation of gender equity at the FBI Academy made seven recommendations to improve the FBI's training of new Special Agents and Intelligence Analysts. Six remain open as of August 2023.

Watch IG Horowitz Speak on the OIG's Report on Gender Equity in the FBI Training Process for New Special Agents and Intelligence Analysts at the FBI Academy.

Hiring

To hire a talented workforce that reflects our nation's diversity, DOJ faces the challenge of using all available hiring authorities and innovative recruitment techniques to compete with other federal agencies and private sector employers. DOJ faces the related challenge of ensuring the integrity of its hiring practices.



OIG analysis of OPM data

Source: Fedscope.opm.gov 2022–2023, all DOJ, Occupation 2210 Technology and Management age, last accessed September 21, 2023

Recruiting and Hiring Top Talent in Competition with the Private Sector

DOJ, and the federal workforce more broadly, are confronting challenges in hiring and retaining skilled employees, especially in the information technology and cyber sectors. The U.S. Government Accountability Office's February 2023 report on OPM's efforts to close government-wide skills gaps noted that these skills gaps may result from insufficient numbers of staff, staff lacking the necessary skills to perform their jobs, or both. DOJ's July 2022 Comprehensive Cyber Review highlighted the specific challenge of hiring and retaining cyber experts, a topic that is discussed in the Cybersecurity and Emerging Technology section of this report. Among other things, that review noted that DOJ should consider offering more competitive incentives and salaries and offer specific programs to attract junior cyber hires, like DOJ's new Cyber Fellows Program.

With 45 percent of DOJ's information technology workforce over 50 and only 9 percent under 30 according to OPM data, and remote work becoming more of an "expectation" than an exception for entry-level and junior workers according to testimony from OMB's Deputy Director for Management, this challenge will only intensify.

The Office of the Inspector General (OIG) addressed DOJ human resource deficiencies related to hiring in an August 2021 Management Advisory Memorandum (MAM). The OIG found that DOJ lacked formalized Department-wide guidance for implementing and managing recruitment, relocation, and retention incentive programs; direct hiring authorities; Pathways Programs; and special hiring authorities for veterans. The OIG made four recommendations for improving human resource functions, all of which remain open as of August 31, 2023.

Hiring a Workforce that Reflects Our Nation's Diversity

In the 2 years since the issuance of Executive Order 14035, Diversity, Equity, Inclusion, and Accessibility (DEIA) in the Federal Workforce, DOJ has continued to struggle with the challenge of increasing diversity, equity, inclusion, and accessibility within its ranks. As Executive Order 14035 notes, "A growing body of evidence demonstrates that diverse, equitable, inclusive, and accessible workplaces yield higher-performing organizations." Unfortunately, the Partnership for Public Service's DOJ performance dashboard shows that DOJ faces greater racial and sex disparities across both the SES and non-SES workforce than the federal government-wide average. In addition, the 2022 FEVS results suggest that the Department, like much of the federal government, must improve its commitment to workplace diversity in that 11.8 percent of DOJ employees believed their supervisor was not committed to a workforce representative of all segments of society. However, as noted above with respect to all of the referenced FEVS scores, the Department also performed lower on this measure than the government-wide score.

FBI Linguists

Source: FBI

DOJ's periodic plans and reports show that DOJ aims to meet this challenge. According to DOJ's 2022–2026 Strategic Plan, as part of efforts to promote good government, DOJ will update its guidance, best practices, and policies related to outreach, recruitment, and hiring, and use data to help ensure diversity and equity in the hiring process. DOJ's 2023–2026 Enterprise-wide Strategic Framework for Equal Employment Opportunity commits to cultivating and retaining a highly qualified and diverse workforce. DOJ's DEIA Strategic Plan includes similar goals. DOJ has also addressed this challenge through new programs. DOJ's FY 2021 Annual Performance Report described a successful new program, the Diversity and Inclusion Dialogue Program. Since its inception in 2014, 917 employees from 26 components have successfully completed the program. DOJ's Special Emphasis

Programs continue to analyze data, identify barriers to recruiting and hiring a diverse array of candidates, and develop solutions to eliminate these barriers. Department leadership has articulated its commitment to diversity, but as the above-referenced data shows much remains to be done to address this challenge.

Compliance with Hiring Laws, Rules, and Regulations

Through our audit and investigative work, we have observed the challenges facing the Department in complying with federal hiring laws and regulations, and its own policies. For example, in August 2023, the OIG released a MAM finding that the Drug Enforcement Administration had hired Special Agents and others who had not successfully completed polygraph examinations, and had allowed Task Force Officers who had failed such examinations to remain on task forces. Additionally, our prior audit work has identified components improperly using contractors to hire individuals to perform inherently governmental functions. Further, our investigations have identified individual cases of hiring misconduct, including at the FBI and the Drug Enforcement Administration.

According to 2021 U.S. Merit Systems Protection Board (MSPB) survey data, DOJ respondents reported perceptions of hiring-related misconduct at significant rates. In general, the Department scored roughly the same or slightly worse than the government-wide response. The following percentages of DOJ respondents reported that they had either observed or been the victims of the following prohibited practices: (1) favoritism in hiring or advancement (22.7 percent), (2) manipulating a recruitment action to improve someone's chances (15.8 percent), (3) obstructing a right to compete for employment (14 percent), (4) solicitation and consideration of improper employment recommendations (12.3 percent), and (5) trying to influence someone to withdraw from competition (8.1 percent).[7]

The OIG is committed to helping the Department address this challenge. For example, the OIG issued a December 2022 MAM recommending that the Bureau of Alcohol, Tobacco, Firearms and Explosives add a policy addressing the recruitment of friends and relatives to avoid any improper hiring practices. As the federal agency responsible for enforcing the law, including hiring laws, it is critical that the Department itself, and its components, fully comply with them.

Sexual Harassment

Despite significant and important efforts by DOJ leadership to address the issue, the Department continues to face the challenge of reducing sexual harassment among employees. The MSPB has recognized that sexual harassment continues to be a challenge across the federal government, not just at DOJ. In its December 2022 report, MSPB recommended three ways to address this challenge, including establishing policies and practices that make clear sexual harassment and other misconduct will not be tolerated, educating employees on these issues, and holding perpetrators accountable. DOJ can seek to overcome this challenge by continuing efforts across these three categories. According to MSPB's June 2023 research brief regarding sexual harassment in the federal workplace, the percent of male DOJ employees experiencing harassment remained steady from 2016 to 2021 at 7 percent, but the percentage of female DOJ employees experiencing sexual harassment jumped from 16 percent to 24 percent. The OIG's investigations continue to hold accountable those DOJ employees who engage in sexual harassment. For example, the OIG recently issued findings regarding inappropriate conduct by an Assistant U.S. Attorney and

[7] This data does not include DOJ respondents who responded "Don't know/NA."

an FBI Program Analysis Officer. The OIG also found that a then supervisor at the U.S. Marshals Service knew about, but failed to report, sexual harassment of a U.S. Marshals Service intern.

As outlined in last year's Top Management and Performance Challenges report, DOJ continues to address workplace sexual harassment and misconduct. DOJ issued a key memorandum in 2018 setting forth directives to help components enforce the Department's zero-tolerance policy for sexual harassment. A 2021 memorandum further worked to address this challenge by establishing a steering committee to review sexual harassment policies. In 2023, DOJ created a new Sexual Misconduct Response Unit, began developing and implementing new training, and committed to issuing a comprehensive Department-wide sexual misconduct policy. These are important steps that the Department needs to continue to support in order to effectively address this significant challenge.

Sexual harassment in the workplace remains an issue

Source: Prostock-studio/stock.adobe.com

Discrimination

DOJ faces the related challenge of reducing workplace discrimination and ensuring that all Equal Employment Opportunity (EEO) violations are promptly addressed. DOJ EEO data from recent years reveals positive and negative developments. The number of employees who have filed EEO complaints has remained generally steady from FY 2019 to FY 2022 although recent data obtained by the OIG indicates that the number of complaints will likely increase for FY 2023. However, data from FY 2019 to the present reflects that DOJ has become better at investigating complaints within the statutorily required time period since FY 2021. In order to meet this challenge of addressing workplace discrimination, the Department will need to enhance both its prevention and enforcement efforts.

APPENDIX 1: The Department's Response to the Draft Report

CONSOLIDATED MANAGEMENT RESPONSE TO
THE OFFICE OF THE INSPECTOR GENERAL 2023 REPORT ON
TOP MANAGEMENT AND PERFORMANCE CHALLENGES
FACING THE DEPARTMENT OF JUSTICE

The Justice Department's (Department) mission is to uphold the rule of law, keep our country safe, and protect civil rights. In July 2022, the Department released its Strategic Plan for Fiscal Years (FY) 2022-2026, which incorporates this mission and details the Department's strategic goals and objectives for the next four years. The Strategic Plan also sets forth performance measures by which the Department will assess its progress and specifies the Department's agency priority goals for the coming fiscal year.

The Office of the Inspector General (OIG) plays an important role in ensuring that the Department achieves its goals and objectives effectively and efficiently. OIG holds Department personnel accountable for misconduct; upholds vital protections for whistleblowers; and protects the public from waste, fraud, and abuse. As part of this work, and as required by statute, OIG annually identifies what it considers to be the top management and performance challenges facing the Department. This year, OIG identified seven challenges it believes represent the most pressing concerns for the Department:

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

II. Strategic Management and Operational Challenges in the Federal Corrections System

III. Promoting and Safeguarding National Security

IV. Cybersecurity and Emerging Technology

V. Pursuing the U.S. Department of Justice's Law Enforcement Mission While Protecting Civil Rights and Civil Liberties

VI. Improving the Management and Oversight of U.S. Department of Justice Contracts and Grants

VII. Effectively Managing Human Capital

Each of these challenges aligns with one or more objectives included in the Department's Strategic Plan. As discussed in greater detail below, the Department is fully committed to addressing each challenge in the coming years.

I. STRENGTHENING PUBLIC TRUST IN THE U.S. DEPARTMENT OF JUSTICE

Public trust is essential to public safety, and upholding the rule of law is a priority of the Department. That priority is rooted in the recognition that, to succeed and retain the trust of the American people, the Department must adhere to norms of independence from improper influence, of the principled exercise of discretion, and of treating like cases alike. Reflecting the seriousness of that obligation, the Department's Strategic Plan lists "Uphold the Rule of Law" as its first strategic goal. The Department continues to take steps to reaffirm, update, and strengthen policies that further public trust.

The Department recognizes its fundamental obligation to provide facilities that are safe for all 143,698 individuals in Federal Bureau of Prisons (BOP) custody and provide for the rehabilitation, health, and safety of incarcerated individuals; to create a safe and secure work environment for correctional professionals; and to foster an environment of transparency and accountability across federal detention facilities. Under the leadership of Director Colette Peters, BOP is focused on reforming and modernizing agency practices, with an emphasis on accountability, integrity, respect, compassion, and correctional excellence.

In April 2023, BOP's leadership announced its new mission statement: "Corrections professionals who foster a humane and secure environment and ensure public safety by preparing individuals for successful reentry into communities." Along with this new mission statement, BOP's new core values are accountability, integrity, respect, compassion, and correctional excellence. Additional information is included below about the many ways in which BOP is advancing this mission and adhering to its core values.

The Department also fully understands the need to use its investigative tools wisely and consistent with the law. Rigorous compliance and oversight related to the Foreign Intelligence Surveillance Act (FISA) continues to be a priority for the Federal Bureau of Investigation (FBI) and National Security Division (NSD). Starting in 2021, after the Department and the Office of the Director of National Intelligence (ODNI) identified additional compliance incidents involving the FBI's querying of raw FISA information, FBI worked with the Department and ODNI to institute a series of remedial measures to strengthen compliance, including by (i) requiring FBI personnel to affirmatively "opt-in" in order to query unminimized Section 702 information; (ii) ensuring heightened approvals on batch job FISA queries; (iii) supplemental guidance and mandatory training on query requirements; and (iv) new restrictions and oversight of sensitive queries. These measures have significantly strengthened compliance and led to a drop in the number of U.S. person queries conducted. In its most recent opinion, the U.S. Foreign Intelligence Surveillance Court (FISC) found that the FBI is complying with the query standard over 98% of the time. Meanwhile, the FBI saw a 94% drop in U.S. person queries from 2021 to 2022 and a further 41% drop during the first three quarters of 2023. Recognizing that these new systems changes and policies will only remain effective if people follow them, the FBI has also recently introduced accountability measures imposing escalating consequences for query compliance incidents resulting from negligence. Relatedly, the FBI has also implemented a new "Field Office Health Measure" to rate senior leadership on FISA compliance efforts within their field offices.

In response to OIG's findings that FBI personnel fell short of the FBI procedures that require agents to document support for all factual assertions contained in FISA applications to ensure the applications are "scrupulously accurate," known as the "Woods Procedures," the FBI took several steps to strengthen supervisory accountability and the process involved in the Supervisory Special Agent (SSA) review of FISA applications. The OIG identified as a priority responding to its recommendations relating to Woods Procedures, and the many steps taken already by the FBI show that the Department has addressed with urgency the problems the OIG identified. These steps include deploying a new FISA application workflow process platform called the "Bridge," and updating the requirements set forth in its FISA and Standard Minimization Procedure Policy Guide (FISA & SMP PG). In addition, the FBI now mandates that FISA Accuracy subfiles be maintained electronically unless certain limited exceptions apply. As a result, if any questions arise as to the FISA-Designated Case Agent's (FDCA) or supervisor's actions in ensuring accuracy, Sentinel's preservation of comments and the activities in the activity log provide auditors with significant information with which to verify the FDCA's and supervisor's actions.

In light of these reforms, the Department strongly supports reauthorizing Section 702 of the Foreign Intelligence Surveillance Act (FISA) to ensure that its efforts to keep our country safe from cyber, nation-state, terrorist, and other threats remain informed by the most valuable and timely intelligence. Section 702 is an indispensable tool for protecting American national security by permitting the U.S. government to collect foreign intelligence information about non-U.S. persons reasonably believed to be outside the United States.

The Department also remains steadfast in its commitment to ensuring that attorneys maintain the highest ethical standards to foster accountability and public trust. Department attorneys conducting investigations, litigating cases, and providing legal advice must adhere to complex legal and ethical standards and strict rules of professional conduct. For over 48 years, the Department's Office of Professional Responsibility's (OPR) primary mission has been to ensure that Department attorneys perform their duties in accordance with the highest professional standards, as would be expected of the nation's principal law enforcement agency. Because OPR maintains an effective system for investigating attorney professional misconduct and conducts its work independently, the public can be assured that OPR's investigations are not influenced by any relationship with prosecutorial offices or the attorneys whose conduct OPR investigates.

II. STRATEGIC MANAGEMENT AND OPERATIONAL CHALLENGES IN THE FEDERAL CORRECTIONS SYSTEM

As noted in last year's Management Response, OIG's oversight has greatly assisted the Department in carrying out its responsibility to provide a safe, secure, and humane environment for all individuals in Federal Bureau of Prisons (BOP) custody. BOP's new mission statement focuses on fostering a humane and secure environment and preparing individuals for successful reentry. BOP is committed to providing a safe environment for both its employees and the adults in its custody, and the core value of accountability requires BOP leadership and their employees to be responsible and transparent.

Addressing staffing challenges. The Department is working to ensure that all BOP facilities have appropriate staffing levels. Hiring and retention of BOP employees remains critical to provide BOP with the flexibility and stability needed to carry out its mission and to protect the well-being of its dedicated employees and the safety of those in BOP's care. As of September 2023, around 88% of BOP's funded positions are filled. Moving forward, BOP will deploy a hiring strategy that includes a comprehensive, data-driven recruitment campaign. As part of this campaign, BOP will host online recruitment events, launch targeted ad campaigns, and utilize data analytics to gauge the effectiveness of its recruitment and retention strategies.

BOP is also using targeted strategies to recruit high-need, hard-to-fill positions such as Correctional Officers and Health Services Employees. BOP's National Recruitment Office conducts targeted outreach to potential Health Services applicants and recruits through community partnerships. BOP uses special rate tables to pay salaries above applicable locality rates for other hard-to-fill professional positions across its locations, including nurses, physician's assistants, nurse practitioners, pharmacists, psychologists, and medical technologists. In May 2023, BOP received approval to resume its Accelerated Training and Promotion Program for Nurses and Advanced Practice Nurses through at least May 2028. This supplements BOP's existing use of market pay for psychiatrists, physicians, and dentists.

Preventing suicides. BOP continues to address operational challenges that have affected the safety of its institutions, including by enhancing suicide prevention efforts. BOP continuously monitors and tracks research and best practices as it relates to suicide prevention. To that end, a Warden's Advisory Group was launched to review the BOP's current policies and practices related to suicide prevention. Each institution has a Clinical Psychologist designated as a Suicide Prevention Program Coordinator. These coordinators monitor at-risk individuals and guarantee adherence to the Bureau's assessment and intervention protocols. BOP also equips all staff with the necessary training to identify and effectively care for those who are at risk of suicide. Any time a risk of suicide is suspected, psychologists are to swiftly conduct Suicide Risk Assessments. When an individual is identified as a possible risk for self-harm, they are to be immediately safeguarded as the BOP develops short-term and long-term plans for the individual's mental health.

Reducing the unnecessary use of restrictive housing. BOP remains committed to short-term and long-term plans that will advance long-standing efforts to improve behavior modification and limit utilization of the restrictive housing tools in line with research and best practices. In the short term, BOP has activated an internal working group to compare its policies to best practices nationwide. For the long term, BOP and the National Institute of Justice (NIJ) announced a partnership to conduct a comprehensive and rigorous study of the use and impact of restrictive housing in federal correctional facilities. The partnership responds to the recommendations of the Department's *Report and Recommendations Concerning the Use of Restrictive Housing*, which called for more research on the prevalence and effects of restrictive housing and the development of alternatives.

Ending sexual misconduct and strengthening internal accountability. In 2022, the Deputy Attorney General convened a working group of senior Department officials from components with expertise on addressing sexual misconduct. The working group issued a *Report and Recommendations Concerning the Department's Response to Sexual Misconduct by Employees of the Federal Bureau of Prisons*, which identified recommendations from the working group's 90-day review of the Department's response to sexual misconduct by BOP employees. In particular, the Report offered more than 50 recommendations in five areas: prevention, reporting, investigation, prosecution, and administrative discipline. The Deputy Attorney General directed that BOP and other components affected by these recommendations take immediate and concrete steps to implement them. Since the Report's release, BOP has worked diligently to implement the recommendations by preventing employee misconduct before it happens, identifying it quickly when it occurs, and holding those who engage in misconduct accountable. The Deputy Attorney General convened an Advisory Group to ensure that the recommendations are implemented as directed and to address other issues promptly when they occur.

Consistent with recommendations, BOP has reorganized its Office of Internal Affairs (OIA) and moved oversight of the Special Investigative Agents (SIAs) from each correctional institution to BOP Headquarters. Over 60 SIAs who previously reported to wardens now report directly to OIA. BOP has also increased the number of agents and employment attorneys to ensure timely investigations and accountability. For example, OIA has hired over 50 new investigators to investigate employee misconduct. In addition, BOP has assigned onsite SIAs to all female institutions. Cases, caseloads, and case durations are monitored continuously by the BOP Director to increase efficiency in investigations and accountability.

At the same time, BOP continues to work diligently with fellow law enforcement entities, and others to ensure a meaningful investigatory and disciplinary process. Additionally, BOP Director and Inspector General meet regularly, to review the status of cases that are under review as well as open cases. The BOP further recognizes that it is critical that every employee and person in custody knows that they can come forward without fear of retaliation, and if retaliation does occur, that individuals are held accountable for that misconduct as well.

Updating and increasing the coverage of security cameras in BOP institution is an essential element of its efforts to prevent misconduct. The OIG has identified recommendations relating to cameras and facilities issues as a priority, and BOP has taken these recommendations seriously by charting a clear course for solving the identified problems. BOP has updated its comprehensive Strategic Plan for transitioning to a fully digital security camera system to include an estimated timeline to complete the work. BOP is actively expanding the number of cameras in critical areas, which recently included filling an urgent need for an additional 150 cameras at one female facility with previously insufficient coverage. BOP is prioritizing an ongoing review to assess coverage of these systems throughout BOP to eliminate "blind spots" at each institution and identify the number of additional cameras needed to address them.

BOP will continue to use the approximately $16 million in funding provided by Congress for ongoing repair and maintenance requirements for the camera upgrades. This activity is expected to occur yearly, subject to appropriations by Congress. After completing the camera upgrades, the base funding will be used to update cameras relying on older technology and upgrade each facility's Video Management System (VMS).

Lastly, BOP plans to allocate approximately $35 million for cameras using fiber optic cabling in facilities where this cabling is already installed, and for the installation fiber optic cabling in facilities where it is not yet installed to allow for upgraded cameras. BOP estimates that over the next three years it will need approximately $125 million to complete the digital camera installations.

Implementing the First Step Act. The First Step Act (FSA) Annual Report issued in April 2023 includes information responsive to the requirements of Section 3634, which requires a risk and needs assessment system that supports ongoing efforts towards implementing policies required under the FSA. For example, consistent with the FSA's emphasis on transitioning individuals to a community setting, the Department expanded the use of home confinement for individuals who do not pose a danger to the community. BOP also successfully published its First Step Act Time Credits Policy along with two substantive updates in FY 2023. In addition, the BOP issued 14 policy documents in FY 2023. For example, BOP issued a policy instructing employees on procedures for reporting allegations of employee misconduct and for conducting investigations of allegations, as well as a policy on the Bureau's employee assistance program.

The Department also notes that OIG in November 2022 closed its Management Advisory Memorandum (MAM) recommendation regarding policy issues impacting BOP's implementation of the FSA. In its closure memorandum, OIG noted BOP's prioritization of all policies pending negotiation with the national union, including those related to the FSA, and BOP's successful reduction of the backlog of policies pending negotiations.

III. PROMOTING AND SAFEGUARDING NATIONAL SECURITY

The Department is committed to investigating, prosecuting, and otherwise disrupting threats to America's national and economic security. These threats include not just espionage efforts, but also foreign influence operations, economic espionage, and critical infrastructure attacks. Defending American institutions and values against these threats is a national security imperative and a priority for the Department. The Department continues to work with international partners and other federal law enforcement to address these threats.

Countering nation-state threats. With respect to nation-state threats, the governments of the People's Republic of China (PRC), Russia, Iran, and North Korea are becoming more aggressive and more capable in their malign activity than ever before. Last year, the Department announced its broader strategy for countering nation-state threats. That strategy focuses on the areas where the Department's authorities can have the most impact in combating the greatest threats to our national security, including those in the context of transnational repression, foreign malign influence, cyber, espionage, and theft of technology and intellectual property. For example, in July 2023, the Department announced that a

Russian citizen with alleged ties to Russia's Federal Security Service was arrested in Estonia and extradited to the United States to face charges for his involvement in a conspiracy to illegally obtain and provide sensitive, American-made electronics and ammunition in furtherance of Russia's war efforts and weapons development.

The Department continues to address the threats posed by the PRC government and its agents—not the Chinese people or those of Chinese descent, who are often the victims of these crimes. In June 2023, three defendants were convicted on charges of stalking Chinese nationals in the United States and acting as illegal agents of the People's Republic of China as part of a global and extralegal repatriation effort known as "Operation Fox Hunt." In April 2023, the Department arrested two defendants in New York on charges of operating an illegal overseas police station in the United States on behalf of the Chinese government.

In addition, the Department is continuing to take actions in response to Russia's unprovoked continued invasion of Ukraine. As noted in last year's Management Response, on March 2, 2022, the Department launched Task Force KleptoCapture, an interagency law enforcement task force dedicated to enforcing the sweeping sanctions, export controls, and economic countermeasures that the United States, along with its foreign allies and partners, has imposed in response to Russia's unprovoked military invasion of Ukraine. It was designed to help deploy U.S. prosecutorial and law enforcement resources to identify sanctions evasion and related criminal conduct. The Task Force continues to leverage all of the Department's tools and authorities to combat efforts to evade or undermine the collective actions taken by the U.S. government in response to Russian military aggression. Task Force KleptoCapture has seized over $500M in assets in recent cases, including having:

- Filed a civil forfeiture complaint against the luxury superyacht *Amadea*, reportedly worth more than $300 million and tied to sanctioned Russian oligarch Sulieman Kerimov;

- Obtained full forfeiture of $5.4 million owned by sanctioned Russian oligarch Konstantin Malofeyev and, using newly enacted authority, transferred the forfeited funds to the State Department to support Ukraine in remediating the harms of Russian aggression;

- Obtained a guilty plea from a U.S. lawyer who participated in a scheme to make approximately $3.8 million in U.S. dollar payments to maintain six real properties in the U.S. that were owned by Viktor Vekselberg; and

- Indicted and arrested the president of a U.S.-based company and a co-conspirator for allegedly engaging in $150 million in sanctioned transactions for the benefit of a designated Russian oligarch (Sergey Kurchenko). Both defendants subsequently pleaded guilty.

Protecting advanced and emerging technologies. In addition, earlier this year, the Department announced the creation of the Disruptive Technology Strike Force, an interagency team led jointly by the NSD and the Commerce Department's Bureau of Industry and Security that includes federal prosecutors in U.S. Attorneys' Offices around the country, as well as agents from the FBI, Commerce

Department, and Homeland Security Investigations at Department of Homeland Security (DHS). These prosecutors and agents investigate and prosecute companies and individuals who violate U.S. laws governing transfer of technology and combine those efforts with administrative enforcement actions and private sector partnership. Since the Strike Force was stood up in February 2023, it has announced 11 cases, a selection of which illustrates the breadth of the Department's work in this field:

- Four cases target procurement networks that were allegedly created to help support Russia's war effort, including by supplying its military and intelligence services. The technology Russia has sought to acquire includes things like microelectronics, sophisticated military testing equipment, and quantum cryptography, and, in multiple cases, Russia has illegally funneled the technology through transshipment points in places like Hong Kong and Cyprus.

- In one case, the Department charged a Chinese national for violating U.S. sanctions laws by attempting to sell to Iran materials used to produce weapons of mass destruction. The defendant tried to arrange the sale using two Chinese companies that the U.S. government has sanctioned for supporting Iran's ballistic missile program.

- Another case charged a Russian-Tajikistan dual national living in New York for conspiring with two Russian nationals who live in Canada to send millions of dollars' worth of electronic components to entities in the Russian technology and defense sectors.

- Two other charged cases involve former software engineers who allegedly stole software and hardware source code from U.S. technology companies in order to market it to Chinese competitors. The stolen information includes trade secrets used by the U.S. companies to develop cutting-edge AI technology, including self-driving cars and advanced technology used to manufacture parts for nuclear submarines and military aircraft.

IV. CYBERSECURITY AND EMERGING TECHNOLOGY

Managing cyber-related threats and emerging technologies presents an evolving and difficult challenge. In recent years, malicious cybercrime—from both nation-states and cybercriminals—has posed an increasing and constantly evolving threat. The Department has taken a comprehensive approach to cybersecurity.

As noted in last year's Management Response, in July 2022, the Department released its Comprehensive Cyber Review report. The Comprehensive Cyber Review made a series of Department-wide recommendations, many of which the Department has now adopted or is in the process of implementing. Among its recommendations, the Review recommended: (1) the creation of the National Cryptocurrency Enforcement Team (NCET) within the Department's Criminal Division to focus on combating illicit uses of cryptocurrency; (2) the launch of the Civil Cyber-Fraud Initiative (CCFI) by the Department's Civil Division, which leverages authorities under the False Claims Act to pursue civil actions against government grantees and contractors who fail to meet cybersecurity obligations; and (3) the development of a new Cyber Fellowship within the Department, designed to foster a new generation

of prosecutors and attorneys equipped to handle emerging cybercrime and cyber-based national security threats.

Moreover, the Department has adopted a new approach to cyber-based investigations that prioritizes disruption of persistent cyber threats alongside traditional criminal charges and arrests. Examples of disruptive actions taken by the Department include: (1) seizures and searches of domains, command-and-control (C2) servers, and other infrastructure owned or operated by criminals; (2) use of court-authorized orders to remove or disrupt malicious software so as to prevent additional attacks and harm to victims; and (3) freezing, seizing, and forfeiting property, including cryptocurrency, derived from or involved in criminal activity.

In just one example of the approach the Department is taking to disrupt cyber threats, in January 2023, an international ransomware network responsible for extorting and attempting to extort hundreds of millions of dollars from victims in the United States and around the world was dismantled. Known as the "Hive" ransomware group, this network targeted more than 1,500 victims since June 2021 and targeted critical infrastructure and some of our nation's most important industries. Before seizing two back-end computer servers used by the Hive network earlier this year, the FBI provided decryption keys to over 300 victims around the world who were actively under attack, helping to prevent approximately $130 million in ransom payments.

To continue to meet the threat posed by state-sponsored cyber actors, the Department's NSD created a new National Security Cyber Section. In line with the Department's greater emphasis on disruption efforts, the National Security Cyber Section is prioritizing efforts beyond arrests and prosecutions to include disruptive actions earlier in our investigations against the individual actors and key nodes in the cybercrime ecosystem that enable those individuals. In addition to being a response to the Department's Comprehensive Cyber Review, the new section is an integral part of the Implementation Plan for the President's National Cybersecurity Strategy.

The Department has also continued to take steps to enhance its own cybersecurity. In response to the data security breach in February 2023, the United States Marshals Service (USMS) remediated the immediate risk exposed by the incident by retiring the compromised system and then reconstituted capabilities by enhancing existing USMS systems and by implementing new USMS systems that employed best practices and the Department's Zero Trust cybersecurity tools. The USMS coordinated with the Department's Office of the Chief Information Officer to ensure transparency of planned and implemented IT security measures. In addition, the USMS ensured the new systems were entered in the Cyber Security Assessment and Management application and prepared Initial Privacy Assessments for review and approval by the USMS Senior Component Official for Privacy and the Office of Privacy and Civil Liberties. In light of this incident, the Deputy Attorney General led a Department-wide review of component information technology systems to ensure appropriate cybersecurity was in place and to correct issues before any vulnerability could be exploited.

V. PURSUING THE U.S. DEPARTMENT OF JUSTICE'S LAW ENFORCEMENT MISSION WHILE PROTECTING CIVIL RIGHTS AND CIVIL LIBERTIES

In all its efforts, the Department is guided by its commitment to protecting civil rights and civil liberties. This is reflected in the Department's Strategic Plan, which reiterates the Department's commitment "to a whole-of-Department approach to protecting civil rights and reducing barriers to equal justice and equal enjoyment of the rights, privileges, and immunities established by the Constitution and laws of the United States."

Building trust in law enforcement. The Department is committed to working with its partners in communities and police departments across the country to advance the accountability, transparency, and public trust that are essential to public safety. Pursuant to Executive Order 14074, *Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety*, the Department is working to establish a National Law Enforcement Accountability Database, a centralized repository of information documenting instances of federal law enforcement officer misconduct. The Department is also assisting the International Association of Directors of Law Enforcement Standards and Training (IADLEST) with expanding and upgrading its existing National Decertification Index (NDI), which is a national registry of certificate or license revocation actions relating to state and local officer misconduct.

In May, the Department, led by the Community Oriented Policing Services (COPS) Office, finalized the first-of-their-kind accreditation standards to help further encourage state, local, Tribal, and territorial law enforcement agencies to adopt policies consistent with those highlighted in the Executive Order. The Department also released a Strategic Plan for supporting the goals of the Federal Interagency Alternatives and Reentry Committee, which was established by the Executive Order. The goals include safely reducing criminal justice system interactions, supporting rehabilitation during incarceration, and facilitating reentry for individuals with criminal records.

In addition, each year, the Department provides billions of dollars in federal financial assistance and requires recipients of this funding to comply with Title VI of the Civil Rights Act of 1964 and the nondiscrimination provisions of the Omnibus Crime Control and Safe Streets Act. The effective implementation and administrative enforcement of federal civil rights laws is of vital importance to the Department. The Office of Justice Program (OJP)'s Office for Civil Rights (OCR) is responsible for ensuring that funding recipients from all Department grantmaking offices comply with these federal laws that prohibit them from discriminating against individuals or groups of individuals in employment or the delivery of services or benefits because of race, color, national origin, sex, religion, or disability. OJP's OCR has taken several steps to enhance its internal processes and expand the office's capacity. Additionally, OCR has worked to increase the public's awareness of how and where to file civil rights complaints and how to access informational resources and other tools. Of note, in June 2023, OCR launched a redesigned website that gives the public online access to file civil rights complaints with the Department's Civil Rights Division (CRT) through a centralized portal. In addition, OCR and CRT

established a Memorandum of Understanding (MOU) to ensure strategic coordination and information sharing.

Combating violent crime. As the OIG report notes, combating violent crime is a longstanding and significant priority for the Department. In May 2021, the Attorney General announced the Comprehensive Strategy for Reducing Violent Crime, which focused on data-driven approaches to preventing, detecting, and prosecuting violent crime and on areas in which federal law enforcement agencies and resources can act as force-multipliers for state and local partners. In the 30 months since that strategy was adopted, the FBI, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the Drug Enforcement Administration (DEA), and USMS have all undertaken geographically targeted enforcement initiatives designed to surge resources to communities at the greatest risk of gun violence, organized crime, and gang activity.

In addition, focused prosecutorial initiatives by the Criminal Division and the U.S. Attorneys' Offices—such as the Houston Violent Crime Initiative—are using all available federal statutory tools, including the Racketeer-Influenced and Corrupt Organizations Act, to convert those enforcement actions into criminal judgments. And the Department's sharing of federal resources—such as community policing grants and access to crime-gun intelligence—has built up capacity among state and local law enforcement partners and resiliency within the communities they serve.

Tackling the opioid epidemic, including fentanyl. As noted in the OIG report, according to the Centers for Disease Control and Prevention, there were approximately 110,000 fatal overdoses in 2022, and fentanyl is the leading cause of death for Americans between the ages of 18 and 45. These deaths are tragic, and the Department has been tackling the opioid epidemic along a number of fronts. This effort includes marshalling and coordinating resources both within the Department and with other federal agencies, state, Tribal, and local law enforcement partners, and foreign governments. The Department's components—notably the DEA, the FBI, the Criminal Division, the Civil Division's Consumer Protection Branch, and U.S. Attorneys' Offices—target every aspect of the fentanyl supply chain, from the chemical companies manufacturing fentanyl precursors to the network of illicit labs producing the deadly drug to the traffickers smuggling it and then peddling it to unsuspecting consumers and finally to the sophisticated money-launders who enable it all.

Through its One Pill Can Kill campaign, the DEA also is working to alert the American public of the dangers of fake prescription pills. Already in 2023, the DEA has seized a record 62 million fentanyl pills, which already exceeds last year's total of 58 million pills.

As the Attorney General recently stated when announcing eight indictments relating to fentanyl trafficking against China-based chemical manufacturing companies and employees, fentanyl is the deadliest drug threat the United States has ever faced. The Department's agents and prosecutors are working every day to get fentanyl out of our communities and bring to justice those who put it there.

Protecting vulnerable communities from abuse and exploitation. The Department takes seriously its obligation and its commitment to protecting the most vulnerable among us, including

children. To provide clearer guidance on when FBI personnel must alert law enforcement of suspected abuse, the FBI revised the Domestic Investigations and Operations Guide (DIOG). These efforts were in response to a series of OIG priority recommendations that identified gaps in the way the FBI coordinated with state and local authorities on allegations of crimes against children. The revisions clarify that all FBI personnel have a mandatory obligation to report suspected abuse of children, the elderly, and other vulnerable individuals, and sets forth specific documentation and process requirements for personnel to follow to ensure proper notifications are made.

The Department's FY 2024 budget request also includes $5.1 million and 14 positions (11 agents) for the FBI's Combating Crimes Against Children program that are specifically intended to respond to OIG's findings. The FBI plans to develop a Crimes Against Children Unit (CACU) for East (E) and West (W) regions of the United States to be housed at FBI headquarters, to enhance Resiliency and Safeguarding Resources, and to increase the Child Exploitation Operational Unit's (CEOU) Special Agent staffing. Developing the program management and training structure will better enable the FBI to follow OIG's recommendations. The creation of the headquarters regional program management units will afford the FBI the ability to provide more resources to the field and have more visibility and control of active investigations.

VI. Improving the Management and Oversight of U.S. Department of Justice Contracts and Grants

The Department awards billions of dollars in grants each year and is committed to ensuring these awards are managed effectively. The Department is working to address the challenges to proper contract and grant management identified in the OIG report. The Department's grantmaking components view their fiduciary responsibility to effectively administer grants as a top priority. All three grantmaking components work to continuously improve and strengthen their policies and procedures, risk management strategies, and oversight and monitoring efforts. The Department fulfills its grant oversight duties through direct communication with grantees, the review of progress and financial reports, programmatic and financial monitoring, grantee audit resolution, training and technical assistance, and targeted support to higher risk grantees.

Ensuring the effective and proper distribution of grants. OJP continues to take steps to ensure proper administration and oversight of its contracts. In its report, the OIG notes that the Department continues to face the challenge of effectively managing its grant portfolio, which is complicated by the need to prevent and detect fraudulent activity. To address this challenge, OJP conducts pre- and post-award risk assessments designed to identify and mitigate risk of errors, fraud, waste, and abuse. The risk assessment process allows OJP to: (1) review the potential risk presented by applicants; and (2) select which grantees receive in-depth monitoring based on level of risk to federal dollars. In addition, OJP continues to conduct financial and programmatic monitoring of all its state administering agencies on a risk-informed four-year rotation.

With advancements in its data analytic capabilities, OJP has access to real time performance metrics at the grant, grantee, and program level, which allows for more effective oversight to inform

training and technical assistance efforts for internal staff and/or funding recipients. This includes providing guidance and clarification to internal staff on monitoring grant recipients' compliance with subrecipient management and validating performance data to source documentation.

OJP also carried out a robust solicitation process for the procurement of JustGrants contract support consistent with the Federal Acquisition Regulation procurement policies and procedures in awarding the Blanket Purchase Agreement. Currently, JustGrants is operational and functioning and supports over 46,000 users, managing over 22,600 grants totaling $27.5 billion. Since the launch of JustGrants, the Department's grantmaking components have awarded 16,547 grants totaling over $15 billion. Over the last three years, OJP's Office of the Chief Information Officer, in partnership with the OJP program and business offices, the COPS Office, and the Office for Violence Against Women (OWV), has worked to identify, triage, and address the most urgent functional gaps and make overall program and system improvements. Using key performance data and feedback from users, OJP is continuously assessing and enhancing the JustGrants system functionality and usability, the effectiveness of training resources, and responsiveness of system support services.

Strengthening the Crime Victims Fund. Regarding management of the Crime Victims Fund (CVF), OJP takes seriously its responsibility to ensure fiscal accountability for all recipients. OJP's Office for Victims of Crime (OVC) provides annual grants to eligible state victim compensation programs and, through the CVF, reimburses states 75% of what they award to victims of crime. OVC has taken numerous steps over the last several years to address the risks associated with the size of the CVF, such as prioritizing in-depth monitoring of these awards; reviewing risk-indicator reports to proactively identify and resolve potential issues; and assessing adequacy of subrecipient monitoring policies, procedures, and practices of all CVF grantees. Of the over $4 billion that the OIG has audited since FY 2015, 0.3% has resulted in questioned costs.

VII. Effectively Managing Human Capital

The Department recognizes that it can only accomplish its mission of upholding the rule of law, keeping our country safe, and protecting civil rights if it has a dedicated, high-skilled, and diverse workforce. The Department's EEO Strategic Framework for 2023-2026 was recently approved by the Acting Assistant Attorney General for Administration and the Department EEO Officer, with a commitment to four major goals that will: (1) ensure compliance with regulatory mandates of a model EEO program; (2) educate and engage the workforce; (3) cultivate and retain a highly qualified and diverse workforce; and (4) leverage data and technological innovation. The Department continues to work towards meeting these goals.

The Department's Diversity and Inclusion Dialogue Program was launched in 2014 as a pilot program, and in 2021, it expanded to include the participation of employees in Department field offices located across the United States. Since its inception, 917 employees from 26 components have successfully completed the program. The Department's Special Emphasis Programs continue to analyze workforce data, identify potential barriers to employment, and develop and implement strategies to eliminate barriers, including employment outreach, training, and professional development activities.

As the OIG report notes, the Department's periodic plans and reports show that it aims to meet the challenge of increasing diversity, equity, inclusion, and accessibility within its ranks.

In September 2023, the Deputy Attorney General announced the findings of the Sexual Harassment Steering Committee that she empaneled to review the Department's sexual misconduct policies and evaluate whether they serve the needs of the Department's workforce. The Steering Committee gathered and assessed relevant policies across the Department, held discussions with internal and external experts, examined best practices and efforts undertaken in other agencies and in the private sector, reviewed results of focus groups and a survey designed by the Steering Committee, and examined data on sexual misconduct from the Department, the EEOC, and the U.S. Merit Systems Protection Board. The Steering Committee also consulted with the OIG, as well as with law enforcement and other large components about their reporting and investigation practices, tracking processes, victim services resources, discipline systems, and training programs.

The Steering Committee offered 11 recommendations to improve the Department's handling of sexual misconduct allegations, understanding that the Department's efforts to fully assess and address sexual misconduct must be ongoing, and the Deputy Attorney General accepted these recommendations and immediately began to implement them. The Deputy Attorney General directed the creation of a Sexual Misconduct Response Unit (SMRU) and hired its Director. Among other responsibilities, the SMRU will serve as a centralized unit responsible for developing, managing, and executing a comprehensive sexual misconduct policy applicable across the entire Department. In addition to being a resource for receiving sexual misconduct complaints, the SMRU will monitor component-led investigations (other than those conducted by the OIG) and disciplinary actions in sexual misconduct matters to ensure they are unbiased, fair, and effective, and will have the authority to conduct its own investigations in certain circumstances. To enhance transparency, the SMRU will gather information about investigations and discipline and submit a semi-annual report to Department leadership.

* * *

The Department appreciates OIG's work in helping to improve our transparency, productivity, and effectiveness. Components across the Department are addressing the numerous findings, conclusions, and recommendations contained in the specific reports and audits that the OIG report discusses. The Department looks forward to continuing its cooperative relationship with the Inspector General on those matters and on future audits, investigations, and reviews.