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

Top Management and Performance Challenges Facing the Department of Justice–2024

October 10, 2024

Memorandum For: The Attorney General
The Deputy Attorney General

From: Michael E. Horowitz
Inspector General

Subject: Top Management and Performance Challenges Report

Attached to this memorandum is the Office of the Inspector General's (OIG) 2024 report on the top management and performance challenges facing the U.S. Department of Justice (the Department or DOJ), which we have identified based on our oversight work, research, and judgment. We have prepared similar reports since 1998. By statute, this report is required to be included in the Department's Agency Financial Report.

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

1. The Ongoing Crisis Facing the Federal Corrections System,
2. Strengthening Public Trust in the U.S. Department of Justice,
3. Promoting and Safeguarding National Security,
4. Cybersecurity and Emerging Technology,
5. Pursuing the U.S. Department of Justice's Law Enforcement Mission While Protecting Civil Rights and Civil Liberties,
6. Strengthening the Administration and Oversight of Contracts and Grants, and
7. Managing Human Capital.

While these challenges are not rank ordered, we believe that it is critical that the Department address the escalating strategic management and operational challenges facing the federal correction system, which is beset by deteriorating facilities, staffing challenges, and concerns over institutional safety and security and healthcare. The serious issues identified during recent OIG unannounced inspections of Federal Bureau of Prisons facilities, including significant facility issues affecting the conditions of inmate confinement and operational deficiencies in core inmate management and security functions, have heightened concern about

the Department's ability to fulfill basic mission requirements. Strengthening the public's trust also remains vitally important for the Department, as confidence in the Department as an institution and its employees is essential to fulfilling the Department's mission to uphold the rule of law, keep our country safe, and protect civil rights.

Additionally, the Department must continue to promote and safeguard national security as it works to counter acts of terrorism and violent extremism, hold international criminal networks accountable for crimes, and ensure the nation's elections are secure and free from foreign influence. Increasingly sophisticated cyber criminals and the rapid advancement of emerging technologies such as artificial intelligence, will require the Department to enhance its cybersecurity strategy and better safeguard sensitive data and information systems. The Department will also need to continue carefully balancing its responsibility to keep the American people safe against its responsibility to protect civil rights and civil liberties. And, as the Department strives to protect communities against violent crime, opioids and other narcotics, and child exploitation, it must also ensure that adequate oversight and accountability measures over law enforcement are robust and effective.

To maximize taxpayer dollars, the Department must continue to ensure that the management of DOJ contracts and grants comply with federal law and requirements. Lastly, the Department's ability to hire and retain top talent next year and beyond will depend, in part, on (1) addressing pay disparities between the federal workforce and the private sector; (2) managing workplace flexibilities to maintain operational readiness while being responsive to work-life balance needs; (3) implementing succession planning to address the shifting generational make-up of the federal workforce and retain institutional knowledge; and (4) quickly and appropriately addressing allegations of sexual harassment and discrimination.

The OIG publicly posts a monthly report on its website listing all outstanding recommendations and identifies its highest priority recommendations on oversight.gov, a website hosted by the Council of the Inspectors General on Integrity and Efficiency that features Inspector General oversight reports and information from across the federal government. The OIG's priority recommendations are those the OIG believes, when implemented, will have the most benefit or impact to DOJ's mission, operations, programs, or funds. Factors we consider when identifying priority recommendations include (1) monetary impact; (2) reduction to waste, fraud, abuse, or misconduct; (3) impact on program efficiency and effectiveness; (4) impact on health, safety, national security, or the economy; (5) current value to policy makers; and (6) the recommendation's relationship to a high-profile area such as OIG top management challenges, agency strategic priorities, Council of the Inspectors General on Integrity and Efficiency top challenges, congressional interest, and global or national emergencies.

In this report, we highlight in text boxes the OIG's three current priority recommendations to increase awareness and emphasize the importance of quick and effective implementation of these important improvements.

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

Challenge 1: The Ongoing Crisis Facing the Federal Corrections System

Among the most important challenges facing the U.S. Department of Justice (the Department or DOJ) is the long-standing crisis facing the Federal Bureau of Prisons (BOP). As Inspector General Michael Horowitz detailed in congressional testimony earlier this year, these recurring, chronic problems have been well over a decade in the making. Indeed, over the past 20 years, the OIG has issued over 100 reports detailing these serious systemic issues facing the BOP. The Office of the Inspector General's (OIG) oversight reports have identified recurring issues that impede the BOP's efforts to consistently ensure the health, safety, and security of all staff and inmates within its custody. Last year, the Comptroller General for the first time added the BOP to the U.S. Government Accountability Office's high-risk list due to its "long-standing challenges with managing staff and resources, and planning and evaluating programs that help incarcerated people successfully return to the community." Addressing these challenges at the BOP will not only require the sustained and serious attention of the BOP Director and the Department leadership, but also of the Office of Management and Budget and Congress.

Among the many challenges facing the BOP is its persistent inability to address staffing shortages in key positions, lack of sufficient funding to repair its crumbling infrastructure, and the introduction of contraband at its prisons. These staffing, infrastructure, and contraband issues have seriously compromised the safety and security of staff and inmates. The BOP has undertaken BOP-wide efforts to determine the staffing needs of its facilities, how its salary structure impacts its ability to recruit and retain employees, and the amount of funding it needs to repair and maintain its facilities.

Another particularly serious challenge facing the BOP, and the Department, is the continuing problem of sexual assault of inmates by BOP personnel. The OIG continues to dedicate significant investigative resources to these cases, as evidenced by our ongoing investigative efforts at Federal Correctional Institution (FCI) Dublin, where the Warden, Chaplain, and other staff have been convicted on sex abuse charges. The OIG's investigation at FCI Dublin demonstrates what can happen when misconduct is not timely identified and addressed, and instead spirals and poisons the culture of an institution. The Department has taken several important and positive actions in an effort to address these issues, including the Deputy Attorney General's convening of a working group to review the BOP's and DOJ's response to sexual misconduct by DOJ personnel; in November 2022, the Working Group issued a report that contained numerous recommendations and reforms, which the OIG supports. Further, the Deputy Attorney General has repeatedly emphasized to U.S. Attorneys and federal prosecutors the importance of prosecuting sexual assault cases, as well as other criminal actions by BOP employees, including contraband smuggling. This has led to an increase in the number of OIG investigations being accepted for prosecution—which both ensures accountability for those BOP employees who engage in wrongdoing and sends an important deterrent message to BOP staff that engaging in criminal activity can result in a felony conviction and sentence of incarceration.

In FY 2024, the OIG focused its non-investigative resources on oversight of the BOP through unannounced inspections of nine institutions, as well as audits and evaluations of institutional safety, BOP programs, contracts, and facilities. The OIG's unannounced inspections program conducted inspections at FCI Sheridan, FCI Lewisburg, and Federal Medical Center Devens, as well as the food services operations at six BOP institutions. Additionally, the OIG published an Evaluation of Issues Surrounding Inmate Deaths in Federal Bureau of Prisons Institutions, which detailed the serious contributory risks that contribute to suicides of inmates and need to be addressed, including poor communication, contraband, and lack of information, and issued a Management Advisory Memorandum (MAM) in which we highlighted concerns about the BOP's use of temporary secure enclosures with limited space for long periods of time. Other oversight of the BOP that the OIG conducted this past year included a review of the BOP's contract with the American Correctional Association to obtain reaccreditation, which we found did not add value or improve the BOP's operations and programs. The BOP has since ended its contractual relationship with the American Correctional Association for accreditation and reaccreditation services.

On July 25, 2024, the Federal Prison Oversight Act was signed into law. The Act, which the OIG supports, seeks to improve BOP oversight by expanding the OIG's risk-based inspections of the BOP's correctional facilities and establishing an independent BOP Ombudsman to receive and investigate complaints.

OIG Ongoing Work: Inspections of Six BOP Facilities–Food Service Operations

Following up on our findings during an unannounced inspection last year at FCI Tallahassee, in June 2024, we conducted six unannounced, concurrent inspections of food services operations at the following BOP institutions:

1. U.S. Penitentiary McCreary, Kentucky;
2. Metropolitan Correctional Center Chicago, Illinois;
3. Federal Correctional Complex Allenwood, Pennsylvania;
4. Federal Correctional Complex Pollock, Louisiana;
5. FCI Marianna, Florida; and
6. FCI Mendota, California.

We expect to report on those inspections during the first quarter of fiscal year (FY) 2025.

Source: OIG May 2023 and June 2024

Widespread Staffing Shortages

As we have consistently seen through our oversight work, understaffed prisons with overburdened employees create security and safety issues. We have repeatedly found, including during our unannounced inspections at FCI Waseca, FCI Tallahassee, FCI Sheridan, and FCI Lewisburg, that significant Correctional Officer (CO) staffing shortages have a cascading effect on institution operations, often requiring substantial use of overtime, including mandatory overtime, and the temporary reassignment of non-CO staff to work in CO posts (a practice known as augmentation). This use of augmentation affects the ability of these non-COs to conduct their routine duties, which include performing maintenance and teaching inmate programs, including First Step Act programs. Moreover, the routine use of overtime—whether voluntary or mandatory—can negatively affect staff morale and attentiveness and, therefore, institution safety and security.

In February 2024, the OIG issued a report evaluating inmate deaths in BOP institutions and found that one particularly serious consequence of the BOP's staffing shortages was an impairment of its ability to reduce the risk of inmate deaths. In particular, the report detailed how the understaffing of Health and Psychology Services positions limited an institution's ability to provide treatment and programs that can help mitigate the risk of inmate deaths. The OIG found that the use of augmentation or overtime to compensate for staff shortages overburdened existing staff and potentially contributed to staff fatigue, sleep deprivation, decreased vigilance, and inattentiveness to duty. Similarly, the OIG's unannounced inspection of FCI Tallahassee detailed how healthcare staffing shortages at that facility negatively affected inmate healthcare treatment. Similarly, the OIG's unannounced inspection of FCI Sheridan in November and December 2023, identified glaring healthcare staffing shortages that resulted in a substantial backlog of healthcare treatment.

In a report issued by the BOP in April 2023, the BOP described strategies to address staffing issues, including its reliance on augmentation and overtime. Among other things, the report described a contract awarded by the BOP in June 2021 to produce a system-wide staffing assessment, as well as targeted hiring campaigns and recruitment incentives. The BOP reported that the contractor was scheduled to complete the first phase of implementation of an automated staffing tool for Correctional Services in July 2023. The U.S. Government Accountability Office reported that, as of March 2024, the BOP estimated the tool would be fully implemented by October 2024. However, the OIG has identified through its inspections program, concerns expressed by BOP institutional managers with the preliminary staffing levels projected by the contractor's staffing tool. Moreover, we observed significant variations between institutions' currently authorized staffing levels as supplemented by the use of overtime and the projected staffing levels provided by the contractor's staffing tool during our inspection in February 2024; our FCI Lewisburg inspection report discusses these variations. The BOP's ability to effectively address its staffing issues in corrections, healthcare, education, training, facilities, and other areas will continue to be impaired unless and until it can determine how much staff it actually needs at each of its facilities. Similarly, the BOP's ability to recruit and retain staff will be impaired until it can determine the salary scale that is needed to attract talented individuals to work in its institutions.

Crumbling Infrastructure

Evidence of water intrusion from the roof, with plastic covering a single-level housing unit ceiling during FCI Tallahassee inspection

Source: OIG, May 2023

The BOP continues to struggle with management and oversight of its facilities. As of February 2024, the BOP estimated that the major repairs needed across its facilities would cost $3 billion. During an OIG audit, we determined that all 123 of the BOP's institutions required maintenance—finding, among other things, multiple facilities with seriously damaged and leaking roofs—and that conditions at three of its facilities had so substantially deteriorated that the BOP determined they had to be partially or fully closed. Further, we found that the BOP lacks a well-defined and comprehensive infrastructure strategy, which impacts its ability to plan for repairs and communicate needs to Executive Branch leadership and to Congress. The BOP does not have adequate funds to maintain its facilities because each year the Executive Branch requests a facilities budget for the BOP that is grossly inadequate to meet the BOP's needs. For example, the total budget DOJ requested for the BOP in FY 2025 was $8.809 billion, which was comprised of $8.549 billion for Salaries and Expenses and $260 million for Buildings and Facilities expenses. The request for Buildings and Facilities expenses, which includes funds for both new construction and for modernization and repair, is woefully lacking in view of the BOP's estimate that it needs $3 billion for major infrastructure repairs. Moreover, we determined that this amount is well below the recommendation by the Federal Facilities Council to fund federal facilities maintenance programs at a minimum of 2 to 4 percent of their current replacement value on an annual basis, estimated to be $675 million to $1.3 billion in FY 2022.

Following our reporting last year as a result of inspections, audits, and evaluations on the crisis presented by the crumbling infrastructure at BOP institutions, the OIG has continued to find serious infrastructure and facilities issues during inspections at FCI Tallahassee, FCI Sheridan, and FCI Lewisburg that negatively affect the conditions of confinement. Specifically, the OIG found at FCI Tallahassee that some inmates in the female prison lived in housing units in which water frequently leaked from ceilings and windows on or near their living spaces. The OIG also observed poor conditions inside communal inmate bathrooms. According to Facilities Department staff, roofs covering inmate housing units at the female prison routinely leak and roofs covering all five of the general population inmate housing units needed to be replaced. At the time of the OIG inspection, FCI Tallahassee had requested and received approximately $3.6 million to replace windows in two of its housing units and to replace the roofs covering its administration building, education building, and Special Housing Unit building at the female prison. While these are necessary repairs, FCI Tallahassee had not yet requested or received funding to replace roofs covering the five general population housing units at the female prison. The OIG's inspection of FCI Lewisburg also found

infrastructure issues at the institution, including significant damage to the institution's food service area as well as the need to replace much of the institution's fire alarm system. BOP officials estimated the cost to address infrastructure issues at Lewisburg is more than $28 million.

At the time of the OIG inspection of FCI Sheridan, Facilities Department staff told us that many of the institution's systems, including its heating and cooling systems, are approaching the end of their projected lifespan and need to be updated. They estimated the cost of this work to be $21.6 million. FCI Sheridan requested funds from the Western Regional Office to address these issues, however, due to the BOP's limited budgetary resources for infrastructure repair and replacement, the request was unfunded at the time of the OIG inspection.

Contraband

As identified in the OIG's report on inmate deaths in federal custody, contraband drugs and weapons pose a significant risk to the health and safety of inmates, appearing to contribute to nearly one-third of the inmate deaths in our scope across the BOP from FYs 2014 through 2021. Common contraband items in BOP institutions include illicit drugs, such as synthetic cannabinoids, buprenorphine, and naloxone. Other contraband may be introduced through inmates who serve on work crews, e.g., sanitation and landscaping, outside the secure perimeter and have greater access to vast areas that abut public roads and lands, as was the case at FCI Tallahassee, where inmates were able to collect contraband from the area around the perimeter fencing while out of view of correctional staff. Additionally, contraband is often introduced into the secure correctional environment via unmanned aerial systems (drones), which can carry payloads up to 35 pounds.

Review of the BOP's Contraband Interdiction Efforts

Our 2016 review of the BOP's efforts to prevent the introduction of contraband into federal prisons found that the recently implemented staff search policy was not effective enough to be a deterrent for staff introduction of contraband. Accordingly, we recommended that the BOP develop uniform guidelines and criteria for conducting random staff pat searches across all institutions that require a minimum frequency and duration for search events to ensure that appropriate numbers of staff on each shift are searched with appropriate frequency. The BOP concurred but has yet to provide an updated policy sufficient to close this priority recommendation and three other recommendations from the 2016 report to strengthen the staff search policy.

Source: June 2016

The OIG has repeatedly highlighted insufficiencies in BOP staff searches of inmates. The OIG noted that at FCI Tallahassee, a women's institution, searches are rarely completed in part because the institution does not have enough female staff to conduct searches of female inmates, as required by the Prison Rape Elimination Act. This is just one more example of the cascading effect of the BOP's ongoing staffing challenges. There also have been numerous additional instances throughout the BOP in which staff did not appear to have followed or fully executed certain correctional policies and procedures to identify and interdict contraband. As a result, the OIG also has a long-standing priority recommendation for the BOP to develop uniform guidelines and criteria for conducting random staff pat searches across all institutions that require a minimum frequency and duration for search events to ensure that appropriate numbers of staff on each shift are searched with appropriate frequency.

The OIG also has long recommended that the BOP upgrade cameras at its facilities for video surveillance. Security camera infrastructure technology in a prison environment is critical for monitoring inmate activities, including unauthorized behaviors, and preventing acts of violence, escape attempts, or the introduction of contraband. The presence of cameras serves as a deterrent to violence and allows for quick intervention should an incident arise. The OIG has found that deficiencies within the BOP's security camera system have affected the OIG's ability to secure prosecutions of staff and civilians in BOP contraband introduction cases, and these same problems adversely affect the availability of critical evidence to support administrative or disciplinary action against staff. For example, the OIG inspections at FCI Tallahassee revealed insufficient numbers of cameras, numerous blind spots, poor night-vision, poor zoom quality, and shortened retention periods for video footage. The OIG also observed that digital video recording equipment would only retain footage for a 14-day period in some instances. A 14-day recording timeframe does not allow for investigative follow-up should an incident occur that requires further examination and investigation. Staff at FCI Tallahassee told us that some allegations are reported more than 14 days after the incident has occurred. In other institutions such as FCI Sheridan, the OIG was able to review video footage that was captured 2 months prior to our inspection. Greater consistency is needed throughout BOP institutions with respect to video recording capabilities.

MAM: Notification of Needed Upgrades to the BOP's Security Camera System

In a separate 2021 MAM, the OIG identified critical security lapses with the BOP's security camera system in relation to its coverage, functionality, and storage capabilities. The OIG recommended that the BOP develop a comprehensive strategic plan for transitioning to a fully digital security camera system that, among other things: a. identifies enhancements needed to address camera functionality and coverage deficiencies, b. provides cost projections and the BOP appropriations account to fund the upgrades, and c. includes an estimated timeline for completion of the work. This priority recommendation remains open.

Source: October 2021

Congressional passage of the Prison Camera Reform Act of 2021 was an important and positive step in addressing this problem and the BOP is making efforts to upgrade equipment and coverage system-wide; however, progress has been slow.

Challenge 2: Strengthening Public Trust in the U.S. Department of Justice

Although polling shows that public trust in the federal government has increased modestly in the last year, strengthening public trust in the U.S. Department of Justice (the Department or DOJ) remains a significant challenge. While political polarization has contributed to allegations across Presidential administrations that Department officials take actions that are politically motivated, the Department can help ensure the public's confidence that its actions are based on the facts and the law, not political considerations, by fortifying and adhering to Department policies and holding its personnel to the highest standards.

Ensuring that the Department is Free from Political Influence

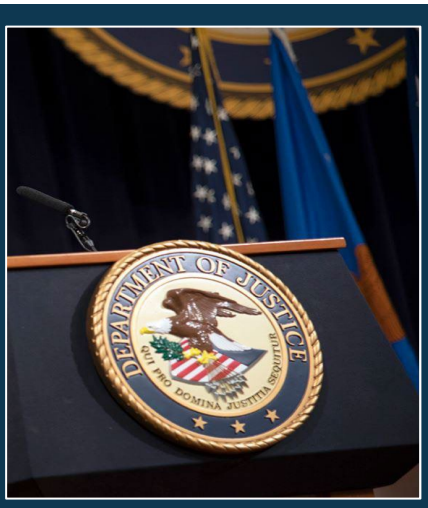


Image of DOJ's podium

Source: DOJ

It is vital that the Department and its employees strictly adhere to policies and procedures designed to protect the Department from accusations of political influence or politically-motivated application of the law. The Office of the Inspector General (OIG) published a report regarding public statements by a U.S. Attorney about an ongoing criminal investigation into alleged ballot tampering during the 2020 Presidential election. The content of such public statements, which included investigative details contrary to Department policy and practice, gave rise to allegations that the announcements were motivated by political considerations. The OIG's investigation found that the U.S. Attorney violated Department policies when he released a letter to county officials about the ongoing criminal investigation. As a result, the OIG identified several steps the Department should take to avoid such issues in the future. The OIG recommended that the Department: (1) strengthen its policy to further clarify that the information Department personnel can include in a public statement about an ongoing investigation is limited to only what is necessary to reassure the public that the appropriate law enforcement agency is investigating a matter or to protect public safety; (2) clarify whether the Department's policy regarding media statements about ongoing investigations applies to the Attorney General; (3) determine which of two apparently conflicting Department policies on the Attorney General's authorities on such media statements is in effect; (4) require the Department to document when requests are made to the Attorney General or Deputy Attorney General, and approvals are issued, for the release of information about investigations that would otherwise be prohibited from disclosure; and (5) consider revising its White House communications policy to clarify what information can be disclosed to the White House in situations where the policy permits communication about a contemplated or pending civil or criminal investigation. Although all five recommendations remain open, the Department is making progress in addressing the concerns highlighted in this report.

One recent OIG investigation illustrated how the unusual substantive involvement by senior Department political appointees in an ongoing prosecution's sentencing proceeding—even when that involvement is permissible and not prohibited by any law or policy—can create the appearance that the Department may not be independent from political influence. The OIG investigated whether political interference caused the Department to file a revised sentencing memorandum and recommendation in the case of a former associate of then President Donald Trump. We did not find evidence that filing the revised sentencing memorandum was the result of improper political considerations. However, the OIG noted how the involvement of the then Attorney General and other high-level Department officials in the preparation and filing of a second sentencing memorandum in a case against the then President's political ally affected the public's perception of the Department's integrity, independence, and objectivity, and that Department political appointees need to exercise discretion and judgment when considering whether to personally involve themselves in DOJ criminal prosecutions.

Similarly, the OIG's Review of the Department of Justice's Response to Protest Activity and Civil Unrest in Washington, D.C. in Late May and Early June 2020 in the aftermath of the killing of George Floyd similarly identified certain actions by Department officials that gave rise to a perception of political influence. For example, while we found that then Attorney General Barr did not order the clearing of Lafayette Park and H Street, and that he did not impact the timing of the clearing operation conducted by other agencies, his public appearance at the park and a statement provided to the media by a Department spokesperson about the Attorney General's role contributed to confusion and inaccurate perceptions. In the same review, the OIG found that Department leadership deployed the Department's law enforcement components without sufficient attention to whether those personnel were properly trained or equipped for their assignments. In doing so, Department leaders placed the safety of the Department's personnel and members of the public at risk, thereby jeopardizing the public's perception and confidence in the Department.

White House as seen from Lafayette Park, Washington

Source: Lee/stock.adobe.com

Last year, an 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 a U.S. Attorney to attempt to influence the outcome of a local partisan election and attended a partisan political fundraiser. 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 political influence.

Addressing Employee Misconduct

When DOJ employees fail to uphold their oaths of public service it erodes the public's trust. Therefore, it is critically important that the Department ensure accountability when its employees engage in criminal or administrative misconduct. In its most recent Semiannual Report to Congress, the OIG reported that investigations in the first half of fiscal year (FY) 2024 resulted in 72 administrative actions, 35 convictions and pleas, 32 arrests, and 28 indictments of DOJ employees, contractors, and grant recipients. Pursuing prosecutions and appropriate sentences in these cases serves to demonstrate the Department's commitment to the integrity of its workforce. Moreover, the Department's components must be vigilant to ensure that employees do not entirely escape accountability by resigning or retiring from government service. In 2021, the OIG conducted a Review of the Federal Bureau of Investigation's (FBI) Adjudication Process for Misconduct Investigations. In that review, the OIG found that when an FBI employee under an internal administrative misconduct investigation separated, the FBI terminated its internal investigation without making findings, even when the investigation was concluded but the employee resigned or retired before discipline could be imposed. We recommended that the FBI ensure that every misconduct investigation is completed, regardless of whether the subject separates, and that it should maintain a written memorandum for each misconduct case documenting a substantiation decision and the supporting evidence when an employee separates from the Bureau while the investigation is ongoing. As of November 2024, these recommendations remain open.

Misconduct among employees of the Federal Bureau of Prisons (BOP) continues to be a significant challenge. In the first half of FY 2024, the OIG opened 85 investigations of BOP employees, and made 139 referrals of alleged BOP employee misconduct to the BOP's Office of Internal Affairs. In last year's, Top Management and Performance Challenges report, we highlighted our ongoing work at Federal Correctional Institution (FCI) Dublin and across the BOP to address sexual misconduct by employees. The Department has appropriately increased its focus on addressing sexual abuse of inmates, and the OIG's Interdisciplinary Team has supported those efforts by providing information, data, and briefings to Department officials and assisting the Department with developing training for investigators and prosecutors. As we describe in a March 2023 report, the BOP plans to hire additional staff to investigate employee misconduct, in an effort to remedy a backlog of investigations and adjudications. These efforts must continue to improve public confidence in the BOP.

Oversight Tools

Protecting whistleblowers from retaliation is critical to the OIG's efforts to detect and prevent misconduct. Every effort must be made to prevent whistleblower reprisal so that DOJ employees are poised to illuminate wrongdoing within their agencies. In May 2024, Inspector General Michael Horowitz expressed concerns in a Management Advisory Memorandum that DOJ lacked conformity with applicable intelligence community policies for protecting whistleblowers who alleged their security clearance has been suspended as retaliation for their protected disclosures. The OIG made five recommendations to the Office of the Deputy Attorney General to address the OIG's concerns. In July 2024, the Department issued a new policy in response to our recommendations that ensures the Department is compliant with whistleblower protections for employees with a national security clearance.

In conducting our oversight work, one common obstacle that the OIG faces are subjects and witnesses leaving the Department during the course of our work. The OIG can subpoena information from third parties and compel interviews of individuals who are currently employed by the Department. However, the OIG does not have the authority to compel interviews of former DOJ employees, DOJ grant recipients, or DOJ contractors, even when the testimony would solely pertain to their actions at DOJ.

As a result, the OIG at times has been unable to obtain valuable testimony from former employees, contractors, or grantees. The lack of testimonial subpoena power impacts our ability to conduct oversight of the Department, including investigations of serious misconduct by Department employees. For example, the OIG investigated whether a then senior official in the FBI retaliated or threatened to retaliate against FBI employees for their participation in an earlier OIG investigation in which the senior official was the subject. The OIG investigation found that the senior official engaged in retaliation, in violation of FBI policy, by making statements about suing employees who the senior official believed provided negative information about the senior official in the earlier OIG investigation. The official made other statements about getting back at one employee for their prior OIG testimony. The OIG investigation also found that the senior official engaged in unprofessional conduct, in violation of FBI policy, by making those statements, by discussing with FBI employees the fact that they were asked to provide testimony to the OIG in the earlier investigation, and by seeking information about that testimony. The senior official resigned from the FBI after providing an initial interview to the OIG at the beginning of the OIG's investigation and later declined a request for a voluntary follow-up interview.

In addition, in our Review of DOJ's Response to Protest Activity and Civil Unrest in Washington, D.C. in Late May and Early June 2020, several key leaders of the Department's response, including the former Attorney General, declined our request for voluntary interviews. Their lack of cooperation led to "significant information gaps…that limit[ed] our ability to determine conclusively what happened [during the events in question]." We have identified the problems associated with this lack of testimonial subpoena power before, including in past Top Management and Performance Challenges and in Inspector General Michael Horowitz's congressional testimony. Both the Department of Defense OIG and the Veteran's Administration OIG have been granted testimonial subpoena authority. The Department's support for the OIG obtaining testimonial subpoena authority would help demonstrate its commitment to hold accountable those who engage in misconduct while DOJ employees.

Another area where public trust in the Department can be strengthened is by giving the OIG authority to investigate allegations of professional misconduct by Department attorneys. This authority is currently vested in the DOJ's Office of Professional Responsibility (OPR); however, unlike the OIG, OPR lacks statutory independence from Department leadership and its leadership is selected by, and can be removed by, the Attorney General and the Deputy Attorney General. The public's trust in the oversight of Department prosecutors would be significantly enhanced by ensuring that this oversight is being conducted by investigators who are outside the supervisory chain of the Attorney General and Deputy Attorney General, and who are free of influence by them. That is among the reasons why Congress has made the OIG statutorily independent of the Department, so the public can trust that the OIG's oversight is being conducted free of influence by Department officials. As Inspector General Michael Horowitz has explained in 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. In an attempt to remedy this problem, the bipartisan "Inspector General Access Act," which would confer this authority upon the OIG, has been introduced in every Congress since 2015. Department support for enactment of the current version of this Inspector General Access Act, S.3813-Inspector General Access Act of 2024, would enhance public confidence in the Department by treating DOJ attorney employees the same as all other DOJ employees, and the same as all attorneys employed at other federal agencies.

Use of Sensitive Investigative Authorities and Impact on Civil Liberties

DOJ must balance its investigative authority and capacity with ensuring the protection of Americans' civil liberties. The means by which investigations are conducted and illegal conduct is prosecuted must not infringe on an individual's constitutional rights.

Adhering to and Applying Consistent Standards When Exercising Investigative Authorities

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 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, the Department substantially revised its news media policy in federal regulations in 2022 and in the Justice Manual in 2024. 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 was in place. This review is examining 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 investigations of alleged unauthorized disclosures of information to the news media, potentially by government officials.

Similarly, and as we discuss in more detail in connection with the National Security challenge, in April 2024 Congress enacted the Reforming Intelligence and Securing America Act, which renewed Section 702 of the Foreign Intelligence Surveillance Act. Following numerous violations reported to the Foreign Intelligence Surveillance Act Court, Congress added new restrictions on the ability of FBI personnel to query Section 702 databases for information associated with U.S. persons and required that the OIG complete a review on FBI querying practices within 545 days of the Reforming Intelligence and Securing America Act's enactment. The OIG has begun its work to meet this 545-day reporting requirement.

Challenge 3: Promoting and Safeguarding National Security

The U.S. Department of Justice (the Department or DOJ) has many responsibilities in the national security arena, including prosecuting acts of international and domestic terrorism, countering foreign malign influence, preventing foreign espionage, protecting critical infrastructure from hostile actors, and safeguarding sensitive information and technology. In addition to the difficult challenges presented by these grave responsibilities, the Department must ensure that citizens' civil rights and civil liberties are not improperly compromised in the name of protecting national security.

FBI New York Assistant Director in Charge checks in with one of the field office's Special Agent bomb technicians helping to keep New Year's Eve safe on December 31, 2023

Source: FBI

According to DOJ's strategic plan, one of its key objectives is countering foreign and domestic terrorism, including exploiting, analyzing, and sharing intelligence with its partners and disrupting terrorist actors through prosecution efforts. U.S. persons, facilities, and interests at home and abroad face persistent and increasingly diverse threats from terrorism. The United States also faces increased threats from hostile nation-state actors such as China, Russia, and Iran. Protecting the integrity of U.S. elections from foreign malign influence efforts by or on behalf of these actors has become an important federal government national security priority in which the Federal Bureau of Investigation (FBI) is the key Department contributor. In addition, threats to critical infrastructure is a significant strategic risk for the United States, threatening our national security, economic prosperity, and public health and safety. Nation-states are targeting critical infrastructure to collect information and gain access to industrial control systems in the energy, nuclear, water, aviation, and critical manufacturing sectors. DOJ has identified as a top objective the need to ensure the economic prosperity of the United States by protecting American companies, academic and research institutions, and workers against hostile actors seeking to steal critical and emerging technologies and intellectual property. To that end, the Department maintains countering foreign espionage as a vital interest.

Preventing and Responding to Acts of Terrorism and Violent Extremism

International Terrorism

The October 7, 2023, Hamas terrorist attack in Israel and ensuing conflict in the Middle East have underscored the ongoing significant threat that foreign terrorist organizations pose to U.S. national security. As FBI Director Christopher Wray noted in his testimony to the Senate Committee on Homeland Security and Government Affairs in late October 2023, the attack may serve as an inspiration to those who seek to commit terrorist acts against the United States, and thus "the ongoing war in the Middle East has raised the threat of an attack against Americans in the

United States to a whole other level." Director Wray also noted after the October 7 attack that al-Qaida issued its most specific call to attack the United States in years, and ISIS urged its followers to target Jewish communities in the United States and Europe. In its 2024 Intelligence Assessment, the Office of the Director of National Intelligence further assessed that "[t]he risk of escalation into direct interstate conflict, intended or otherwise, remains high."

Hostage Rescue Team operators train for a close-quarters battle

Source: FBI

In his April 2024 congressional budget testimony, Director Wray identified terrorism—both international and domestic—as the FBI's continued number one priority. While the FBI remains concerned about the ability of foreign terrorist organizations, such as ISIS and al-Qaida and their affiliates, to carry out or inspire large-scale attacks in the United States, he stated that homegrown violent extremists (HVEs) are the greatest, most immediate international terrorism threat to the homeland. The FBI defines HVE as individuals living or operating primarily in the United States who prepare to engage in terrorist activities in furtherance of a political or social objective promoted by a foreign terrorist organization, even if they are acting independently of any direction by a foreign terrorist organization. Director Wray specifically identified lone actors or small cells of individuals who typically become radicalized online and primarily use easily accessible weapons to attack soft targets as the "greatest threat to our homeland." An Office of the Inspector General (OIG) HVE audit report issued in March 2020 included a recommendation that the FBI examine and identify mechanisms field offices can use to revisit subjects of closed HVE assessments that may warrant further action by the FBI, while also ensuring any such mechanisms do not create any legal, policy, and civil liberties implications. In view of the significance of the HVE threat, we believe the FBI would benefit from its continued efforts to completely address this recommendation, which remains open.

Domestic Terrorism and Domestic Violent Extremism

Domestic terrorism and domestic violent extremism (DVE) continue to pose a significant national security challenge as evidenced by the July 13, 2024 attempted assassination of former President Donald Trump at a campaign rally in Butler, Pennsylvania. The FBI is investigating the incident as a potential act of domestic terrorism as it seeks to learn the deceased shooter's motives and determine the sequence of events leading up to the shooting.

In April 2024, Director Wray described two types of DVE actors, racially or ethnically motivated violent extremists (RMVE) and antigovernment or antiauthority extremists, as the top domestic terrorism threat. The Director has further noted the significant increase in domestic terrorism investigations over the last several years. In its most recent threat assessment, the U.S. Department

of Homeland Security (DHS) also described the continued risk that RMVEs pose in the United States, noting several fatal U.S. based attacks and that RMVEs have in some cases improved the quality of their online recruiting tools, potentially inspiring more attacks.

The OIG has conducted oversight work in an effort to assist the Department in addressing this threat. In June 2023, we released an audit identifying gaps in DOJ's strategy to combat DVE actors. The report highlighted coordination challenges within the Department due to the large number of DOJ components involved in addressing this threat. The report included seven recommendations, one of which is closed and six of which are open as of October 1, 2024. One of these recommendations directed the Department to determine how to empower the Domestic Terrorism Unit of the National Security Division to coordinate and provide leadership across the Department on efforts to address DVE. Similarly, the U.S. Government Accountability Office issued reports in February 2023 and January 2024, both of which highlighted the need for improved coordination between the FBI and DHS and better information sharing with stakeholders in the domestic terrorism/DVE context. The OIG also recommended that the Department improve guidance to law enforcement components so that investigations with a DVE nexus are more consistently and properly identified.

Deputy U.S. Marshals conducting Operation Rolling Thunder at Oklahoma City in 2023.

Source: U.S. Marshals Service

The riot at the U.S. Capitol on January 6, 2021, serves as an indication that the charged political climate magnifies the domestic terrorism threat. The OIG's review of the roles and activities of DOJ and its components in preparing for and responding to the Capitol Riot on January 6, 2021, is ongoing. Based on several factors, including ongoing criminal prosecutions and oversight conducted by other entities, the OIG review is focused on the FBI's direction and handling of its confidential human sources (CHS) in the lead-up to and on January 6, and whether the FBI exploited its CHSs and other available information to determine the nature of threats in advance of the electoral vote certification on January 6. In the 40 months following January 6, 2021, the Department has charged more than 1,424 defendants and obtained 820 guilty pleas in connection with the ongoing investigation. Implementing the remaining recommendations from the OIG and the U.S. Government Accountability Office reports would ensure the Department is better coordinated and able to meet the DVE threat while at the same time safeguarding civil liberties.

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

Maintaining security in the U.S. electoral process is vital to our democratic system of government. It is essential that qualified voters can equally participate in public elections and have their votes

counted without fear of discrimination, intimidation, or fraud. In addition to preventative measures against voter suppression, ensuring our elections are secure and free from foreign malign influence and interference is a priority for the Department.

Adversaries use distinctive tactics and techniques to accomplish their goal of disrupting election processes and undermining the public's confidence in our democratic institutions and values. Foreign-generated deepfakes remain a crucial threat for the Department and other government organizations as they can be used to spread misinformation and propaganda. The FBI continues to commit resources to developing approaches to secure election infrastructure against foreign malign influence operations. These adversarial threats include attempts to undermine the legitimacy of the security and integrity of the U.S. elections process, while also increasing negative sentiments toward the election system through influence campaigns. Consequently, the Department maintains its oversight by supervising and prosecuting cases relating to national security, including any cases involving foreign malign influence and interference in elections from global adversaries. In July 2024, the OIG released a report reviewing the Department's efforts to coordinate information sharing about foreign malign threats to U.S. elections. In that evaluation, the OIG found effective communication within and among three DOJ components tasked with sharing case information regarding foreign malign influence directed at U.S. elections, in addition to DOJ components expressing positive views about their information sharing relationships. However, the OIG found that neither DOJ nor the FBI had a specific policy or guidance applicable to information sharing with social media companies regarding foreign malign influence until February 2024.

Countering Foreign Espionage

The United States faces an expanding array of foreign intelligence threats by adversaries such as China, Russia, and Iran that are using increasingly sophisticated methods to cause harm to U.S. interests. For example, the 2022 National Security Strategy sharply noted that the United States is in the midst of a strategic competition with China, the only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to advance that objective. According to a statement by FBI Director Wray, "The PRC is a singular threat because the Chinese Communist Party has essentially dedicated its whole government to seize economic development in the most critical areas for tomorrow's economy."

DHS Investigations and the FBI conduct a search during a Joint Criminal Opioid and Darknet Enforcement team operation in 2021

Source: FBI

Our nation remains a prime target of foreign intelligence gathering efforts in areas such as critical infrastructure, national security information, academia, technologies, and research laboratories. For example, in 2024, a resident of China, along with a Canadian national and Chinese national, conspired to steal trade secrets from their former employer, an American company which spent millions of dollars in the research and development of manufacturing electric vehicles, and sold products developed with the stolen trade secrets. Successful criminal prosecutions of foreign espionage operations, whether

motivated by politics or economics, can deter and hold accountable those engaged in such activity. In addition, FBI intelligence investigations, in coordination when appropriate with U.S. intelligence community agencies, are essential to addressing this challenge.

Use of Sensitive Investigative Techniques and Impact on Civil Liberties

As outlined above, the Department faces many significant national security challenges. It must, however, safeguard civil liberties in addressing the threat. For example, in recent years, the FBI has come under scrutiny for its use of its authorities under Section 702 of the Foreign Intelligence Surveillance Act (FISA).

Section 702 is critical to the Department's national security efforts. It authorizes the targeted surveillance of non-U.S. persons reasonably believed to be located abroad. First enacted in 2008, it was meant to fill gaps in the previously existing intelligence collection authorities included in FISA. Although it does not allow the surveillance and intelligence collection of persons located in the United States or U.S. persons located abroad, communications involving a U.S. person may be captured incidentally by the government. For this reason, there are several internal controls that are designed to "minimize" U.S. person information, including restrictions on when FBI personnel may query databases for information associated with U.S. persons.

However, despite these controls, there have been numerous repeated querying violations that the Department has reported to the FISA Court. These include searches of Section 702 holdings using the names of individuals arrested in connection with civil unrest in May and June 2020, and individuals suspected of involvement in the January 6, 2021, riot at the U.S. Capitol. It also included searches using the names of political donors to a congressional campaign. As a result, Congress and the President highlighted the need to implement reforms that meaningfully enhanced Section 702 safeguards while continuing to preserve its national security benefits.

The debate around these authorities culminated in the renewal of Section 702 with passage of the 2024 Reforming Intelligence and Securing America Act. The law reauthorizes Section 702 for 2 years with new restrictions on queries of U.S. persons. For example, the Reforming Intelligence and Securing America Act requires FBI personnel to obtain prior approval from a supervisor or attorney before conducting a U.S. person query and prohibits involvement by political appointees in approving such queries. It also mandates audits of U.S. person queries and directs the DOJ OIG to issue a report on FBI querying practices within 545 days of enactment. The OIG has begun its work to meet this 545-day reporting requirement.

Challenge 4: Cybersecurity and Emerging Technology

The challenges presented by maintaining cybersecurity and keeping pace with emerging technology are becoming more complex and critically important as the U.S. Department of Justice (the Department or DOJ) continues to store data digitally, utilize software as a service product, and incorporate emerging technologies into processes and systems. Given that the topics of cyber and technology touch upon so many different aspects of the Department's work, this is a multifaceted challenge that needs to be addressed in a way that comprehensively covers the technological, financial, and privacy risks, among other threats. In addition, cybersecurity is a transnational issue. Global collaboration activities include information sharing with foreign partners on current threats and providing cyber training to foreign law enforcement. As highlighted in a U.S. Government Accountability Office (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. The report cited a lack of dedicated resources, difficulties in retaining highly trained staff, and inconsistent definitions of "cybercrime." Continued collaboration, both across the federal government and among U.S. and international partners, will aid DOJ in combatting increasingly widespread and complex cybercrime.

Enhancing Cybersecurity

"Cybersecurity" is the practice of protecting technology and is aimed at preventing cyberattacks or mitigating their impact. The Department has a leading federal role in the government's cybersecurity strategy, as outlined in the May 2024 White House National Cybersecurity Strategy Implementation Plan. The plan includes the strategy to build and enhance collaboration among these five pillars: (1) defend critical infrastructure, (2) disrupt and dismantle threat actors, (3) shape market forces to drive security and resilience, (4) invest in a resilient future, and (5) forge international partnerships to pursue shared goals.

Federal Bureau of Investigation (FBI) Cyber Division

Source: FBI

Cyber Supply Chain Threats

The Department, like many federal agencies, relies on commercially available technology solutions to fulfill its mission, however this makes it vulnerable to the risks and demands of the market. An excellent example of how vulnerable the U.S. infrastructure is to cyber threats could be seen from the cascading effect of the flaw in CrowdStrike's July 2024 software push that shutdown airlines, companies, and government offices across the globe. According to CrowdStrike's root cause analysis, a defect in a content update to its software caused system instability and resulted in the "blue screen of death," which impacted large segments of the global economy, including key components at DOJ.

Cyber supply chain risk management includes identifying risks within the supply chain and managing those risks. When a cyberattack or other event disrupts the supply chain, problems can be significant such as a slowdown or complete stoppage of product delivery. Cyber supply chain threats can occur through suppliers, vendors, or partners and can result in the unauthorized release of sensitive data, malware, theft of intellectual property, among other things.

The Office of the Inspector General's (OIG) July 2022 audit report highlighted supply chain risks, finding that the Justice Management Division 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. Additionally, while the FBI had a more advanced program for mitigating supply chain risk, the FBI needed to improve its key deliverables to better align with intelligence community requirements, enhance both its risk mitigation and continuous monitoring efforts, and better integrate C-SCRM across the organization. The Drug Enforcement Administration did not have a supply chain risk management program at all. Two of the OIG's recommendations to assist the FBI in mitigating supply chain risks remain open as of July 31, 2024.

In April 2024, the National Counterintelligence and Security Center and partners launched a National Supply Chain Integrity Month awareness campaign. Their mission is to urge public and private sector organizations to reinforce C-SCRM programs with acquisition security, cybersecurity, and enterprise security, known as "A.C.E." Five critical technology sectors—artificial intelligence (AI), bioeconomy, autonomous systems, quantum, and semiconductors—have been prioritized by the National Counterintelligence and Security Center with challenges managing threats and risks to complex supply chains.

Combatting Cybercrime and Cyber Threats

Malicious cyber activity is increasing as the barrier of entry for hackers becomes lower each year and threatens the public's safety and our national and economic security. As a law enforcement agency, combatting cybercrime and cyber threats remain among the Department's highest priorities as part of its mission to ensure public safety against threats foreign and domestic. DOJ, through the FBI, is the lead federal agency for investigating cyberattacks and intrusions. Some of the challenges the Department currently faces include threats from ransomware, insider threats, the need for federal and global coordination in combatting cybercrime, and recruitment and retention of 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. The FBI and DOJ Criminal Division's Computer Crime and Intellectual Property Section lead the effort to address cyber intrusions and attacks and in 2023, the Computer Crime and Intellectual Property Section was actively pursuing dozens of the highest priority ransomware groups, and had 108 open ransomware cases.

The Department has had some success in disrupting ransomware operations. For example, in December 2023 the FBI announced it had disrupted the Blackcat, or ALPHV, ransomware group resulting in restoration of over 500 systems that had been victimized. In March 2022, DOJ unsealed two indictments charging four Russian nationals who worked for the Russian government with orchestrating hacking campaigns that included hiding malware inside software updates for industrial control systems used by the energy sector. The FBI and U.S. Cybersecurity and Infrastructure Security Agency announced in June 2023 that the "Clop" ransomware gang used vulnerabilities in file transfer software to conduct large-scale data theft, including from federal agencies and government contractors. The investigative and technological challenges in this continuously changing arena are significant.

In an effort to assist the Department in managing this threat, the OIG conducted an audit to assess the Department's strategy to combat ransomware threats, its response to, and coordination on, ransomware attacks against public and private entities. The OIG made findings concerning the Department's general approach to combatting ransomware attacks. Those findings include that the FBI and the DOJ Criminal Division's Computer Crime and Intellectual Property Section, which lead the Department's ransomware efforts, have prioritized the ransomware threat and allocated existing resources in an effort to maximize their impact. The OIG also identified opportunities for the Department to improve its efforts to combat the ransomware threat and made three recommendations, including that the Department assess the U.S. Attorney's Offices' implementation of the deconfliction policy for ransomware cases to ensure that federal prosecutors have a consistent understanding of the policy and comply with its requirements. The Department concurred with all recommendations.

Enhancement of Cyber Workforce

Recruiting, hiring, and retaining skilled, cyber employees remains a challenge for the Department. The federal cyber workforce, including many DOJ employees, performs vital work, such as protecting government IT systems, networks, and data from the most sophisticated adversaries, as well as critical infrastructure. In July 2023, the White House Office of the National Cyber Director published the National Cyber Workforce and Education Strategy consisting of four pillars: (1) improving the public's cyber skills, (2) transforming cyber education, (3) expanding and enhancing America's cyber workforce, and (4) strengthening the federal cyber workforce. The Department employs talented cyber personnel to respond to, investigate, and disrupt cyber threats—including attorneys, Special Agents, intelligence analysts, computer scientists, data analysts, forensic technicians, and others. With the increasing pace and sophistication of cyber threats, including ransomware and other malicious attacks, it is more important than ever that cyber-related jobs, within the Department and elsewhere in the federal government, are filled with highly qualified personnel. To address this challenge, the Department must leverage flexible hiring practices and workplace flexibilities to recruit and retain capable employees in the highly competitive market for such talent.

Challenges in the Adoption of Emerging Technologies

Advanced and emerging technologies present both opportunities and challenges for the Department. AI and other emerging technologies are being adopted quickly and have the potential to increase government capabilities and efficiency. However, the risks of these new tools must be managed, and DOJ must understand the legal regulations pertaining to these technologies and

comply with them. This evolving landscape presents challenges for the Department to proactively strategize and respond to emerging risks to not be outpaced by technological change.

The Department's 2022 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. The Emerging Technology Board was established in December 2023 with DOJ's first Chief Science and Technology Advisor and Chief Artificial Intelligence Officer to address the challenges that persist within the Department.

AI technology has been at the forefront of emerging technologies and has enormous potential to change the status quo across government and society at-large. The White House identified AI on its list of critical and emerging technologies this year, and issued Executive Order 14110 last year ordering government agencies to hire technical personnel and utilize AI in their work, taking a whole-of-government approach with AI. While the Department has made efforts to adapt to the change in the technological landscape, such as hiring the Department's first Chief Science and Technology Advisor and Chief AI Officer, 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 Department uses some 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. As the use of more advanced AI increases, the Department cannot afford to be reactive to the risks and consequences of AI, as GAO reported in May 2023. The U.S. Department of Commerce, National Institute of Standards and Technology, has issued an initial framework to manage the risks of generative AI this year, but the management of AI risks undoubtedly poses a major challenge to the Department as the technology is new and constantly evolving and the standards and regulations around AI are few and in their infancy.

Emerging technologies, such as AI, will significantly affect DOJ's efforts to uphold the rule of law, keep our country safe, and protect civil rights over time. When utilizing AI models and tools, DOJ must understand that there is currently a lack of robust and verifiable measurement methods for risk and trustworthiness. To prevent the use of AI in ways that are irrelevant and potentially harmful, the Department must identify flaws and vulnerabilities, such as unforeseen or undesirable system behaviors, limitations, or potential risks associated with the misuse of the system. As part of this effort, the OIG is conducting an audit of the Drug Enforcement Administration's and FBI's integration of AI and other emerging technology as members of the U.S. Intelligence Community, with the primary objective of evaluating compliance with requirements related to artificial intelligence and other emerging technologies, as specified in Title LXVII of the fiscal year 2023 National Defense Authorization Act.

According to a study by the GAO, modern devices, systems, and locations generate, retain, and share enormous volumes of data. This includes information collected from the personal devices of government employees, contractors, and family members, as well as online accounts, credit reports,

online searches, and online purchases. According to the FBI, this data can be used to connect people with locations and organizations, for example identifying a person as an FBI agent, or connecting that agent with a location such as an FBI building, known as ubiquitous technical surveillance. In February 2024, FBI Director Christopher Wray described ubiquitous technical surveillance as a method used by adversaries to exploit the digital trail left behind by individuals allowing the adversary to threaten or compromise government sources, operations, and personnel.

New technologies can include new communication technologies, end-to-end encryption of data, and facial recognition technology, and the Department must adapt. The OIG is conducting 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.

Challenge 5: Pursuing the Department's Law Enforcement Mission While Protecting Civil Rights and Civil Liberties

In recent years, the U.S. Department of Justice (the Department or DOJ) has faced increased scrutiny in its mission to uphold the rule of law, ensure safety and security in our country, and protect civil rights. This task has become increasingly technical and complex in the face of the changing landscape of the international drug trade and emerging technologies that require the Department and its officers to adjust their strategies and focus. The challenge is compounded by the imperative to balance these duties while promoting the public's confidence in law enforcement. Ensuring civil rights and accountability in the Department is critical to maintaining public trust and upholding the principles of justice and equality.

Protecting Civil Rights and Ensuring Law Enforcement Accountability

Promoting accountable law enforcement within the Department involves implementing comprehensive measures that ensure transparency, oversight, and adherence to ethical standards. The Office of the Inspector General (OIG) conducts audits of DOJ law enforcement practices, policies, and procedures to ensure compliance with federal standards and identifies areas for improvement. In September 2023, the OIG issued an audit report of DOJ's use-of-force policies within its law enforcement and corrections components and found certain policy gaps related to use-of-force in custodial situations and inconsistent use-of-force policies and practices in their application to task force officers (TFO) and contractors. We also found that there was no mechanism to help ensure components' training programs are consistent, appropriate, or complete. Since the issuance of the report, the U.S. Marshals Service (USMS) has finalized their policies on "no knock" warrant restrictions and disseminated the updates to personnel. In addition, the Federal Bureau of Prisons updated its policies to meet DOJ's intent for the Department's 2022 use-of-force policy to apply to the Federal Bureau of Prisons non-custodial operations and interactions with the public, as well as fully comply with the Department's 2021 guidance on use of restraints and "no knock" warrant restrictions.

USMS–Operation North Star

Source: USMS

Additionally, the Department's Civil Rights Division continues to pursue excessive force and pattern and practice investigations. Between January and June 2024, the Department announced charges, pleas, convictions, or sentences in at least 10 cases involving use of excessive force by state or local law enforcement officers. In June 2024, the Department released findings that the Phoenix Police Department and City of Phoenix, Arizona, engaged in a pattern and practice of conduct that violated the Constitution and federal law, including unjustified uses of deadly force, unconstitutional shootings, and use of neck and compression restraints. During another civil pattern or practice investigation, the Department found that the City of Lexington, Mississippi, and the Lexington Police Department engaged in a pattern or practice of conduct that deprived people of their rights

under the U.S. Constitution and federal law. The investigation determined, among other things, that the police department used excessive force, conducted searches and arrests without probable cause, and violated the rights of people engaged in free speech and expression, including by retaliating against people who criticize the police.

In addition, the OIG is participating in prosecutions of a USMS TFO charged with murder for allegedly using lethal force that resulted in the death of Casey Goodson in Columbus, Ohio, a Federal Bureau of Investigation (FBI) TFO charged with second degree murder in Michigan after he allegedly used his government vehicle to stop a fleeing felon, and multiple USMS TFOs allegedly involved in assaulting two handcuffed juveniles at a residence in Jackson, Mississippi. Ensuring that such investigations into misconduct are conducted promptly and thoroughly, while providing the public with information, will help promote accountable law enforcement.

As directed by Executive Order 14074, the Department launched the National Law Enforcement Accountability Database, a centralized repository of official records documenting instances of misconduct as well as commendations and awards for federal law enforcement officers. The National Law Enforcement Accountability Database is accessible only to authorized users to help determine suitability and eligibility of candidates for law enforcement positions. As required by the Executive Order, on an annual basis, the Department will publish a public report containing aggregated and anonymized data to maintain transparency and accountability. The creation of such a portal will leverage the technology and data on law enforcement activities and make it easier for police departments to avoid hiring officers who have engaged in misconduct for a previous employer.

Targeting Violent Crime

The FBI recently reported that the rate of violent crime decreased nationwide by approximately 3 percent in 2023; however, combatting gun violence continues to be an enduring challenge for the Department, necessitating continued engagement with partners and stakeholders. Moreover, the Department faces the ongoing and evolving challenge of detecting and intercepting illegal drugs trafficked through complex online and international networks. The Department recently declared the disproportionately high rates of violence experienced by Native American and Native Alaskans as priorities, and has taken additional actions to engage with Tribes to better address urgent public safety issues. As outlined in its strategic plan, the Department must continue to work with and enhance partnerships with federal, state, local, and tribal law enforcement partners to prevent and respond to violent crime.

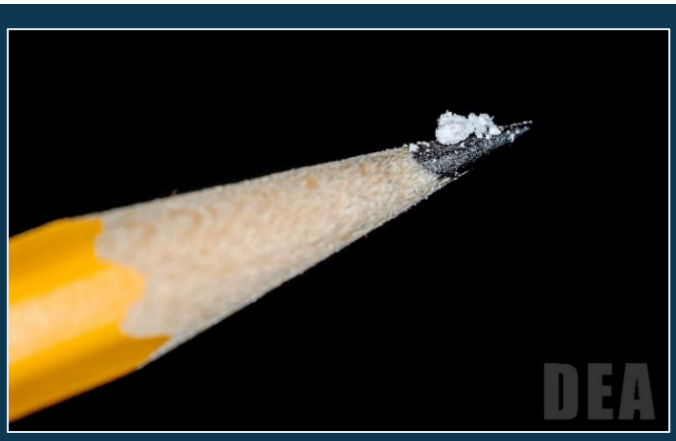
Combatting Gun Violence

The Department identified reducing gun-related violent crime as an Agency Priority Goal within its strategic plan, and committed to focus enforcement efforts on reducing the incidence of guns used to commit violent crime as well as solving more gun-related violent crimes. To assist in the latter goal, the OIG is currently conducting an audit of the Bureau of Alcohol, Tobacco, Firearms and Explosives' (ATF) management of firearm tracing requests used to generate investigative leads for firearms used in crime, known as crime guns. ATF's updated National Firearms Commerce and Trafficking Assessment makes note of many advancements in combatting gun violence, such as the

increased use of crime gun intelligence data. However, the assessment also highlights several emerging issues and challenges, such as the increase of international firearms trafficking and privately made firearm cases. A 2022 National Institute of Justice study found that 77 percent of people who committed mass shootings in the United States between 1966 and 2019 purchased at least some of their weapons legally, while illegal purchases were made by 13 percent of those committing mass shootings. In cases involving K-12 school shootings, more than 80 percent of individuals who engaged in shootings stole guns from family members. The OIG issued an audit report in 2023 in connection with ATF's risk-based federal firearms licensee (FFL) inspection selection processes and administrative actions issued to FFLs. Based on over 10 years of inspection data, the OIG found that ATF had not addressed violations by FFLs in a consistent manner, and it had not always followed ATF policy. Of note, ATF did not often recommend revocation for FFLs with "revocable" violations, such as transferring a firearm to a prohibited person, and some FFLs with repeat revocable violations had been allowed to continue their operations. The Department's attention to the OIG's 13 recommendations to ATF for enhancing oversight of such licensed dealers, 6 of which remain open, could assist in greater diligence by FFLs, thereby preventing ineligible purchasers from obtaining a firearm by apparently legal means.

To facilitate cooperation and partnership in preventing gun violence, the Department has taken several positive steps. For example, it released model legislation to assist states in reducing gun violence and improving gun safety by requiring secure storage of firearms and prompt reporting of lost or stolen firearms. The Department also launched the National Extreme Risk Protection Order Resource Center to provide training and technical assistance to law enforcement, legal, and community partners. Additionally, the Office of Community Oriented Policing Services released a comprehensive Critical Incident Review of the Robb Elementary School shooting in Uvalde, Texas, to identify critical lessons from the law enforcement response and improve future responses in the event of similar incidents in other communities. The report identified several critical failures and other breakdowns prior to, during, and after the Robb Elementary School response and analyzed the cascading failures of leadership, decision-making, tactics, policy, and training that contributed to those failures and breakdowns.

Opioid and Narcotics Interdiction

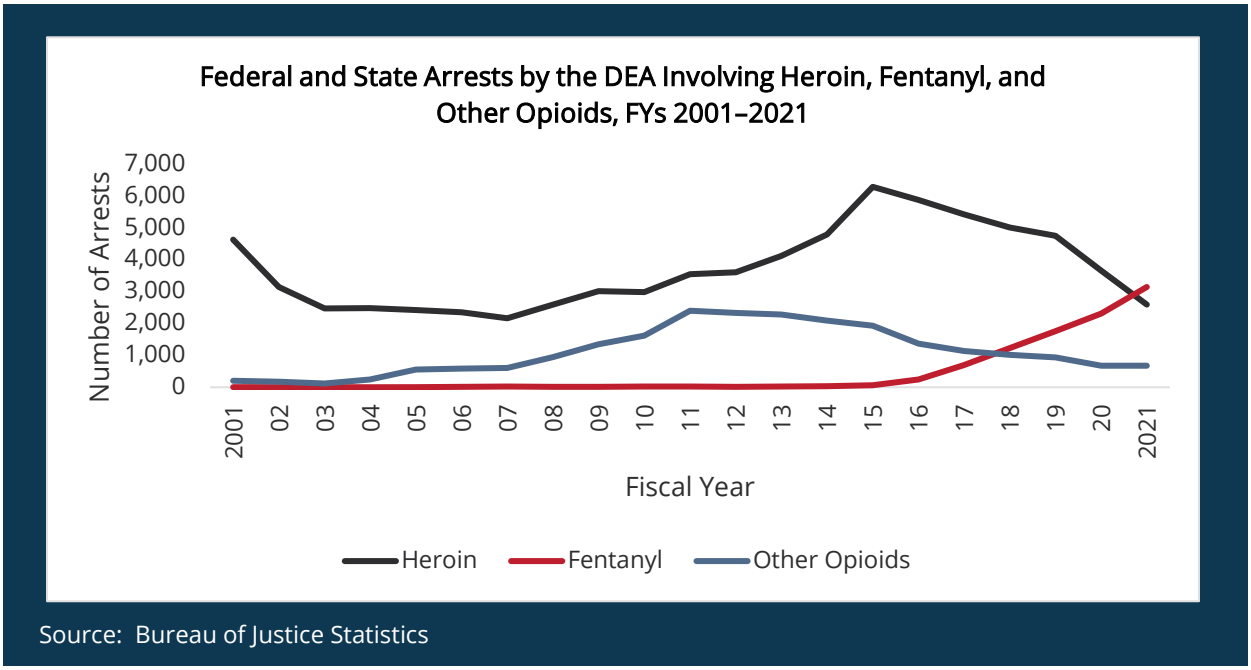


2mg, the amount of fentanyl on the tip of this pencil, can be enough to kill an average American.

Source: DEA

Opioids, particularly fentanyl, continue to pose a challenge not just for the Department, but for the nation. In September 2024, the U.S. Centers for Disease Control and Prevention reported that provisional data show that deaths caused by drug overdose declined by approximately 10 percent over a 12-month period, but nonetheless remain significantly higher than in March 2020. The Department has made numerous efforts to disrupt multi-jurisdictional fentanyl and narcotics trafficking schemes, some with international connections. However, fighting the illegal drug trade, which is driven by international organizations and cartels, presents large-scale and technical challenges, including online and dark web marketplaces. The Department must continue to work closely with domestic and international partner law enforcement agencies to detect and prosecute dark web trafficking schemes that often involve the use of cryptocurrency.

Underscoring the evolving drug trafficking environment, in 2024, the Bureau of Justice Statistics announced that arrests by the Drug Enforcement Administration (DEA) for fentanyl offenses exceeded those for heroin offenses for the first time in fiscal year (FY) 2021. The FBI has similarly highlighted the large number of cases it investigated related to fentanyl trafficking by drug cartels. Additionally, medetomidine has rapidly proliferated in the United States and contributed to mass overdose outbreaks. The Department must continuously work to proactively respond as new and more lethal drugs enter trafficking networks. Moreover, opioid addiction and fatalities continue to plague communities across the country. The Department must be broadminded in implementing its strategy to combat this epidemic.



Source: Bureau of Justice Statistics

As part of its oversight of the Department's opioid, fentanyl, and narcotics efforts, the OIG completed an audit of the Bureau of Justice Assistance Comprehensive Opioid, Stimulant, and Substance Abuse Program, designed to provide financial and technical assistance to entities for comprehensive efforts to identify, respond to, treat, and support those affected by illicit drugs of abuse. The audit found that the Bureau of Justice Assistance can improve its oversight and coordination to ensure the program is achieving its stated outcomes and expanding access to evidence-based drug prevention and treatment, as outlined in the Department's strategic plan. Additionally, the U.S. Government Accountability Office has a priority open recommendation for the DEA to solicit input from licensed distributors of controlled substances and develop additional guidance regarding their roles and responsibilities for monitoring and reporting suspicious prescription drug orders.

Countering the Intensifying Threat of Child Exploitation

Since the beginning of widespread Internet use in the 1990s, the Department has strived to prevent child exploitation and prosecute the offenders. As outlined in the Department's current Strategic Plan, the Department is "determined to make America safer for our young people," via enforcement of current federal laws, to include the PROTECT Our Children Act of 2008, that enable the criminal justice system to hold child exploitation and abuse offenders accountable, as well as collaborating with other federal agencies to address shortfalls in current federal law, improve victims services, providing community education, and improving overall law enforcement response to child abuse and exploitation cases.

In August 2024, as a follow-up to issues identified during the OIG's July 2021 report on the FBI's handling of child sexual abuse allegations against former USA Gymnastics physician, Lawrence (Larry) Nassar, the OIG conducted an audit to evaluate 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. Between October 1, 2021, and February 26, 2023, the FBI opened 3,925 cases that allegedly involved a hands-on sex offense against a child or similar offense, and we reviewed a sample of 327 incidents.

Investigation and Review of the FBI's Handling of Allegations of Sexual Abuse by Former USA Gymnastics Physician Lawrence Gerard Nassar

The investigation and review of the FBI's handling of allegations of sexual abuse by former USA Gymnastics Federation physician, Larry Nassar, identified failures in the FBI's response to the serious allegations by multiple young athletes. The OIG recommended that the FBI reassess its policies to more precisely describe for FBI employees when they are required to promptly contact and coordinate with applicable 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. This priority recommendation remains open.

Source: July 2021

While the OIG found that the FBI has implemented training, policy updates, and system changes to improve its handling of crimes against children allegations upon receipt of the allegations, the OIG identified numerous incidents where FBI employees did not comply with relevant law or policies, including in the following areas: (1) mandatory reporting of suspected child abuse, (2) victim services, (3) transferring incidents between field offices, and (4) responding to allegations of active and ongoing child sexual abuse within 24 hours. For example, we found no evidence that FBI employees complied with mandatory reporting requirements to state, local, tribal, and territorial law enforcement in 47 percent of the incidents we reviewed or to social services agencies in 50 percent of incidents we reviewed. Of the reports that were made, we found that only 43 percent were made within 24 hours, as required by FBI policy.

In addition, we flagged 42 incidents, totaling 13 percent of the incidents we examined, for FBI headquarters review because we believed they may require immediate attention. The types of concerns we identified included: (1) cases that lacked any recent investigative activity or case updates, logical investigative steps, or referrals to appropriate agencies; (2) leads that were not appropriately covered; and (3) instances of substantial non-compliance with FBI policy.

Our audit results demonstrate that the FBI needs to improve its compliance with policies and laws and build upon the FBI's recent changes to its crimes against children and human trafficking program to ensure it appropriately addresses child sexual abuse allegations. The OIG made 11 recommendations to improve the FBI's management of its crimes against children and human trafficking program. The FBI concurred with all 11 recommendations and, prior to the release of the report, took corrective action on two of the recommendations leading to those recommendations being closed.

Combatting and Recovering Pandemic-Related Relief Fraud

As noted in our 2023 Top Management and Performance Challenges report, the COVID-19 Fraud Enforcement Task Force (CFETF) was established by the Department to fight pandemic fraud through coordinated efforts with law enforcement partners. With over 3,500 defendants charged and more than $1.4 billion seized, the CFETF has disrupted transnational criminal networks and domestic offenders. However, despite these accomplishments, the CFETF faces significant challenges.

A major challenge that remains is the statute of limitations to prosecute pandemic-related fraud cases.

Source: Polarpx/stock.adobe.com

One such major challenge is the expiring statute of limitations to prosecute pandemic-related fraud cases (with the exception of cases relating to two programs administered by the U.S. Small Business Administration-, for which the statute of limitations has been extended to 10 years), which will preclude prosecutions not initiated by September 30, 2025. Another challenge relates to resources. The volume of pandemic fraud cases has been overwhelming and requires substantial prosecutorial and investigative resources to pursue. The Department is seeking, in proposed legislation, $300 million to ensure the Department has the necessary resources to prosecute the full range of pandemic fraud, holding accountable the most egregious and sophisticated offenders, and recover additional stolen funds, as well as expand DOJ pandemic fraud "strike force" teams.

The Department faces a difficult road ahead because of the complexity of the fraud schemes and the time it takes to fully investigate and prosecute such cases. DOJ components must assign personnel to COVID-19 strike forces to assist with the development and prosecution of the fraud schemes. In its April 2024 report, the CFETF observed that, "tightening budgets across the federal government make it increasingly difficult to adequately resource CFETF's essential work.".

Protecting Consumers and the Public at-Large from Financial Malfeasance

Technological advances have made the world more interconnected than ever, and the Department faces a rapidly evolving challenge in combatting financial threats against the public. The Department pledged to combat corruption, financial crime, and fraud as part of its strategic plan to ensure economic opportunity and fairness for all, and multiple DOJ components are responsible for prosecuting corporate and white-collar crime. Technology has also increased the opportunity for financial crimes. Among these emerging threats are the use of Artificial Intelligence to commit white-collar crimes such as price fixing, fraud, or market manipulation, and the use of cryptocurrency to defraud victims and launder money.

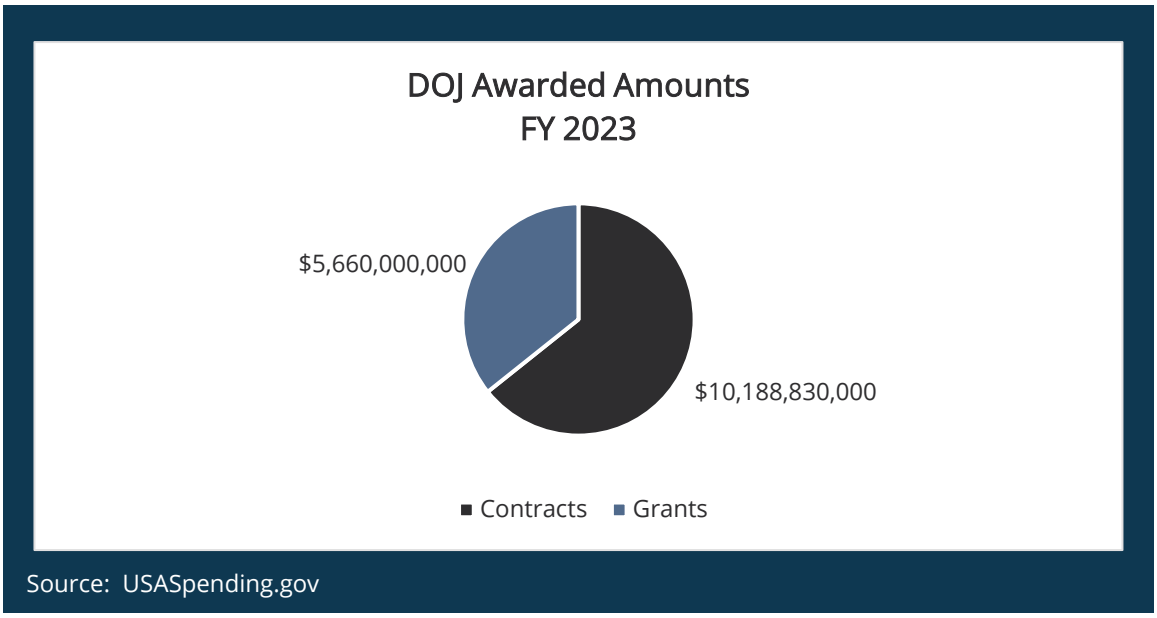
Attorney General Merrick B. Garland Delivers Remarks on Lawsuit Against Live Nation-Ticketmaster for Monopolizing Markets Across the Live Concert Industry

Source: DOJ

As these technologies further develop and advance, the Department must ensure that its enforcement mechanisms stay ahead of, or at least keep pace with, the sophistication of the emerging criminal threats.

Challenge 6: Strengthening the Administration and Oversight of Contracts and Grants

In fiscal year (FY) 2023, the U.S. Department of Justice (the Department or DOJ) awarded over $10 billion in contracts and $5.6 billion in grants. Strengthening the planning, administration, and oversight of contracts and grants continues to be a challenge for the Department as a good steward of taxpayers' dollars.



Specifically, areas of concern for Department acquisition practices include the execution of well-designed procurement plans and cost estimates, monitoring of contractors' performance, and the skills and judgment exercised by the acquisition personnel throughout the procurement lifecycle. Similarly, areas of concern for federal financial assistance, most commonly awarded through grant awards, include monitoring of subrecipients, grant financial management, and program performance.

Contracts

Over the past several years, the Office of the Inspector General (OIG) identified several weaknesses in DOJ's contract management and administration requirements. These include but are not limited to the following systemic issues that the OIG has identified through the audit work:

(1) contracting officials' improper application of contractor cost estimates,

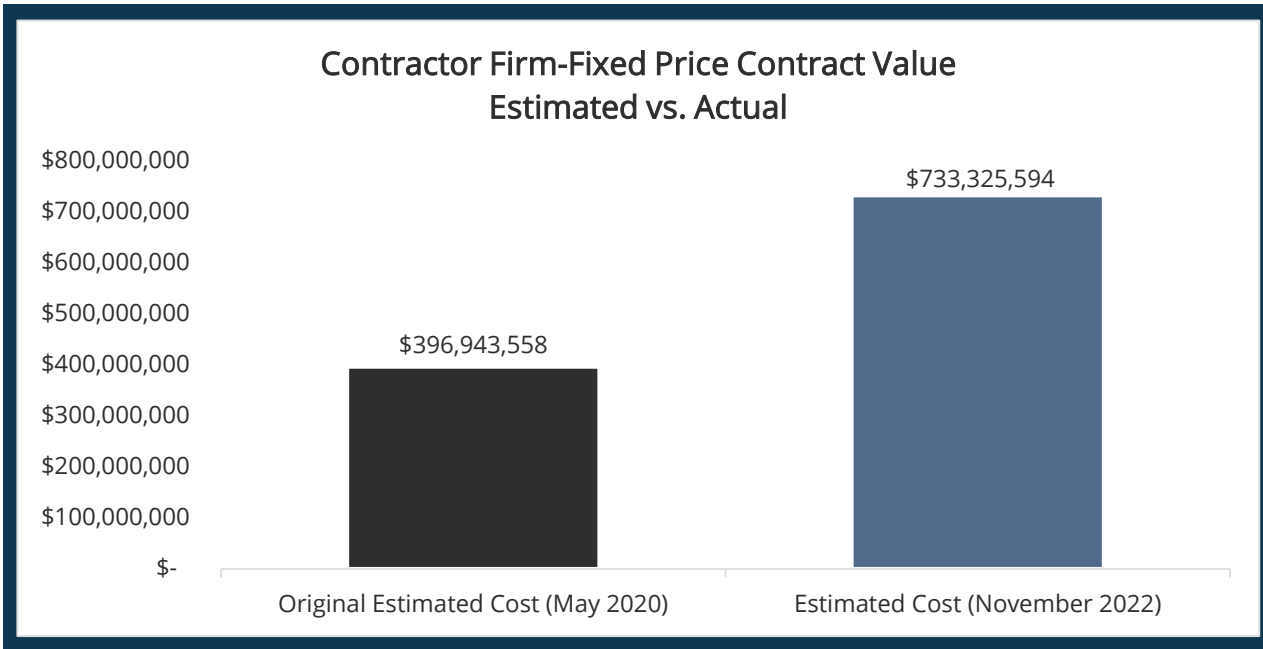
(2) inadequate use of planning documents (e.g., Quality Assurance Surveillance Plans), and

(3) insufficient monitoring of contract performance.

While the Department has taken action to address these recommendations, we have highlighted opportunities for DOJ to improve its compliance with requirements for acquisition planning, administration, and oversight.

Acquisition Planning

Appropriate acquisition planning promotes full and open competition and helps ensure the Department meets its procurement needs in the most effective, economical, and timely manner. The OIG's work reveals that the Department continues to face challenges in the required acquisition planning steps that are necessary to ensure a fair and reasonable price for goods and services. We previously identified the issue of sole-source contracts, awards made without open competition, as presenting elevated risk to the Department in the 2022 and 2023 Top Management and Performance Challenges reports. Similarly, without appropriate planning, firm-fixed-price awards can be problematic. For example, the Bureau of Alcohol, Tobacco, Firearms and Explosives awarded a $396 million firm-fixed-price contract to a contractor for information technology services. Our audit of the contract found that the contractor did not achieve the cost savings it anticipated when program participation level decreased. In the pre-award phase, the contracting official's contract actions did not adequately plan for the cost impact of any reduction in work scope or loss of participants causing increased costs that adversely impacted the Department's budgets. Specifically, DOJ components had to allocate additional money for services that it had planned to be covered under the fixed price. The unforeseen costs resulting from poor acquisition planning also caused contentious interactions between the contractor; the Bureau of Alcohol, Tobacco, Firearms and Explosives; and other participating DOJ components.



The overall task order value increased by $336,382,036 (85%) from the original estimates.

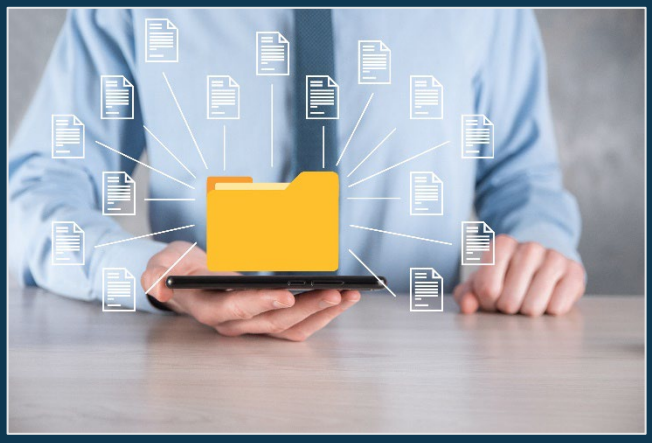
Source: OIG

Another acquisition planning concern is deficient contract practices when selecting sole-source contracts. In an audit of the Federal Bureau of Investigation's (FBI) contract for ballistic research assistant services, the OIG found that the FBI took "unconventional actions" to ensure that the FBI used a specific contractor, did not competitively bid the contract or follow requirements for awarding a sole-source contract, and inappropriately placed the contractor in a personal services role. The OIG also found significant deficiencies in the FBI's management of the contract, including failing to evaluate potential conflicts of interest regarding the contractor's participation in high-value and sensitive FBI procurements, exceeding its authority to extend the contract's period of performance, and applying oversight procedures that were incongruent with Federal Acquisition Regulation requirements for firm-fixed-price contracts. Taken together, the OIG concluded that these issues indicated inadequate contract management and increased contracting risks.

Strengthening the contract acquisition planning process by requiring contracting officials (e.g., Contracting Officers, Contracting Officer Representatives (COR), Contract Specialists), program owners, and contractors to discuss, determine, and agree upon specific cost details and achievable outcomes will increase the likelihood of success of the Department's contracts and reduce unforeseen costs.

Administration and Oversight

Effective contract administration and oversight ensures that the Department receives products and services that fulfill its mission while detecting fraud, waste, and abuse when spending taxpayer dollars. To ensure the Department receives a fair and reasonable price for the goods and services it paid for, the Department should better engage the program and contracting officials throughout the contract lifecycle. Specifically, the Department should aim to provide effective procedures that successfully achieve the contracted needs. For example, an improvement on the development of contract performance measures (e.g., monitoring of unique procurement factors) will help prevent such circumstances.



Effective contract administration and oversight ensures that the Department receives products and services that fulfill its mission while detecting fraud, waste, and abuse when spending taxpayer dollars.

Source: Ivan/stock.adobe.com

Our audits have found that the Department needs to strengthen the COR designation process and the monitoring process. These reports highlighted the need for the components' acquisition offices to correct significant delays and problems arising from the Contracting Officer's untimely issuance of written COR delegations, a role that is critical to the contract administration process and the day-to-day activities of a contract. For example, a COR's authorized delegated functions typically support

the Contracting Officer in ensuring adequate contract monitoring and that the contract requirements are met during the procurement lifecycle.

The Department can make progress in improving its contract management to address this challenge by more clearly designating contract management responsibilities among relevant job functions, using performance metrics, and administering risk-based monitoring tools to help ensure the Department receives the goods and services it paid for.

Grants

The Department continues to face challenges in effectively managing its portfolio of grants. As evidenced in numerous audits of grant recipients, the OIG consistently makes 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 program execution, grant financial management, as well as their oversight of subrecipients of grant funding. With over $5.6 billion in grant funds awarded in FY 2023 alone, the oversight of grants, which has also been identified in nearly every year of the OIG's Top Management and Performance Challenges reports, remains a challenge for the Department.

Grant Programs

More than 200 grant programs are administered by the Department's Office of Community Oriented Policing Services, Office of Justice Programs (OJP), and Office on Violence Against Women. The OIG's oversight helps support the grant-making components administer the programs and recipients use grant funds in a manner consistent with their intended purpose and in compliance with all requirements. These grant programs relate to some of the most critical issues facing the United States today. Therefore, the challenge for the Department in ensuring that the funds are used properly is critically important, and the OIG's oversight is pivotal.

The OIG's oversight ensures that the grant-making components administer the programs, and its recipients use grant funds in a manner consistent with their intended purpose.

Source: Ngampol/stock.adobe.com

For example, the misuse of prescription opioids, as well as heroin abuse, persists as a serious national epidemic. Created as a result of the Comprehensive Addiction and Recovery Act, the Comprehensive Opioid, Stimulant, and Substance Use Program (COSSUP) aims to: (1) reduce opioid misuse and overdose fatalities, and support a variety of opioid-related measures, strategies; and (2) provide financial assistance and technical assistance to identify, respond to, and

support those impacted by illicit drugs. In March 2024, the OIG issued an audit report of the OJP Bureau of Justice Assistance's (BJA) administration of the precursor program of COSSUP, the Comprehensive Opioid, Stimulant, and Substance Abuse Program (COSSAP). The OIG found that BJA did not consistently apply or fully disclose preferences used to evaluate COSSAP applications. BJA's failure to provide notice to all prospective COSSAP applicants of significant evaluation preferences undercut requirements that federal funding opportunities be transparent to maximize fairness of the process, as well as OJP's commitment to ensuring a fair and open process for making awards.

Finally, the OIG has identified recurring findings related to financial management including unsupported and unallowable grant expenditures. For example, an August 2024 audit concluded that the grantee did not maintain adequate supporting documentation for grant expenditures, charged unbudgeted expenses to the grants, did not adequately track its matching costs expenses, and did not use the correct methodology to charge indirect costs to the grants. These failures resulted in the OIG questioning costs in the amount of $247,326 of the $1,555,732 grant funds received by the grantee during the audited period.

Crime Victims Fund

In 1988, the Office for Victims of Crimes (OVC) was authorized by an amendment to the Victims of Crime Act (VOCA) of 1984 to administer the Crime Victims Fund (CVF). The CVF receives monies from fines, special assessments, and forfeited bail paid by people who are convicted of federal crimes in U.S. courts around the country. OVC distributes these funds to (1) state administering agencies (SAA) through the VOCA victim assistance and compensation formula grants and (2) state and local governments, individuals, educational institutions, and private nonprofit organizations through discretionary grants. Congress has allocated $10 million each FY in VOCA funds to the OIG, beginning in 2015, for use in auditing and assessing risks and deficiencies in the management of OVC programs. Since 2016, the OIG has released over 110 reports resulting in about 700 recommendations and approximately $15 million in questioned costs in conducting oversight of the use of these grant funds.

CVF State Administering Agencies

With the CVF funds, SAAs provide pass-through funding to providers of direct services for victims of crime. Such assistance can include crisis intervention, emergency shelter, transportation, legal assistance, and crisis counseling. The OIG has found that the SAAs struggled with monitoring of subrecipients as identified. The purpose of subrecipient monitoring is to ensure that the subaward is being used for the authorized purpose, in compliance with the federal program and grant requirements, laws, and regulations, and the subaward performance goals are achieved.

As an example, a CVF audit issued in March 2024 found that the Arizona Department of Public Safety, which administers the VOCA victim assistance programs that ensure appropriate and accessible services are available to crime victims, had not performed an on-site monitoring visit for all 150 subrecipients who received subawards between FY 2021 and FY 2023. More specifically, 85 subrecipients had not had an on-site Arizona Department of Public Safety monitoring visit in 4 years, and of those 29 subrecipients had not been visited in 10 years. An on-site monitoring visit consists of reviewing supporting documentation related to subgrant financial transactions or performance and evaluating whether a subrecipient's costs comply with VOCA Guidelines, as well as

whether subrecipient performance data reported to OVC was fairly represented, for all subrecipients.

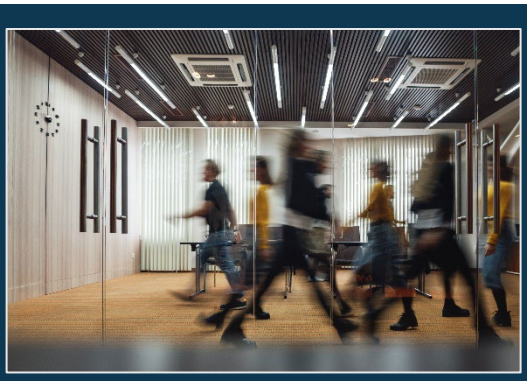
Additionally, SAAs are responsible for the fair treatment of crime victims, including protecting their privacy and personally identifiable information. A CVF audit issued in September 2023 found that the Guam Office of Attorney General (Guam OAG) was not operating its program in compliance with VOCA grant requirements. Specifically, the Guam OAG publicly adjudicated victim compensation claims featuring the public appearance of victims and dissemination of personally identifiable information. As a result, the Guam OAG advocated to change Guam statutes. The Guam Legislature passed Bill 144-37 on July 28, 2023, and the Governor of Guam signed it into law on August 11, 2023. The public law protects victims by allowing the Guam's Criminal Injuries Compensation Commission to have closed meetings to adjudicate victim compensation claims.

Subrecipients

Our CVF subrecipient audits identified concerns with grant financial management and program performance. Grant financial management helps ensure compliance with financial guidelines, general accounting practices, and fiscal management of grant expenditures, all of which can reduce the risk of fraud, waste, and abuse. The OIG identified issues with subaward expenditures in several recent audit reports, including those issued in November 2023, April 2024, and February 2024. Another CVF audit issued in February 2024 found that the University of Maryland Prince George's Hospital Center, a subrecipient of a CVF award to the Maryland Governor's Office of Crime Prevention, Youth, and Victim Services, did not have adequate internal controls to ensure the appropriateness of personnel charges (e.g., timesheets, activity reports, or time-and-effort reports) and to provide evidence of the distribution of costs or allocation of time among various activities.

In a May 2024 CVF audit report, the OIG found that the grantee, a subrecipient of a CVF grant awarded to the New Jersey Department of Law and Public Safety, expended only a portion of funds provided and achieved less than expected under one of the audited subawards because, according to grantee officials, they experienced challenges in the early stages of deploying a new initiative. The OIG also found that the grantee lacked programmatic policies and procedures, including protecting victim personally identifiable information, and performance data reported reflected agency-wide data as opposed to only VOCA-funded services. The OIG's recommendations in these grant audits highlight our goal to help the Department's grant-awarding components and grant recipients comply with Department and other federal regulations and ensure that the funds are efficiently and effectively administered for their intended purposes.

Challenge 7: Managing Human Capital



DOJ relies on talents and skills of its workforce of over 110,000 employees.

Source: leonidkos/stock.adobe.com

The U.S. Department of Justice (the Department or DOJ) relies on the talents and skills of its workforce of over 110,000 employees to accomplish its mission to enforce the law and defend the interest of the United States, ensure public safety against threats foreign and domestic, provide federal leadership in preventing and controlling crime, seek just punishment for those guilty of unlawful behavior, and ensure fair and impartial administration of justice for all Americans. The U.S. Government Accountability Office (GAO) first identified strategic human capital management within the federal government as a high-risk area in 2021. The Department's strategic management of its human capital is important to ensure that the Department meets its performance goals and effectively executes its mission in the most efficient manner. Areas of key concern related to human capital management include recruiting and retaining highly skilled and diverse staff, succession planning and knowledge management, and promoting employee engagement.

Strategic Workforce Planning

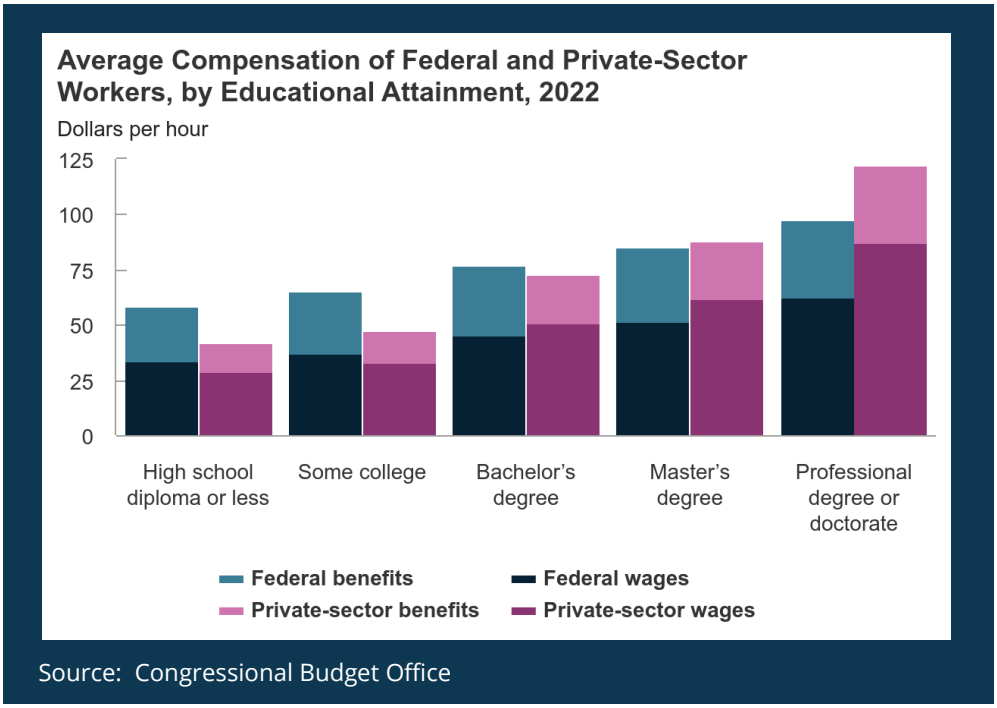
The Department's strategic workforce planning aims to ensure that the agency effectively recruits, develops, and retains a highly skilled and diverse workforce capable of meeting its mission-critical goals. By aligning human capital strategies with organizational objectives, the Department seeks to enhance operational efficiency, foster a culture of continuous improvement, and adapt to evolving challenges. This comprehensive approach underscores the Department's commitment to upholding justice, safeguarding national security, and serving the American public.

Recruiting and Hiring Top Talent in Competition with the Private Sector

Agencies within the Department face competition from the private sector as higher salary and levels of workforce engagement make private sector positions more attractive to new and established professionals. There is a critical need to ensure the Department maintains the high-quality of its workforce so that it is capable of meeting the Department's critical mission.

Pay disparities between the federal workforce and private sector have notably impacted the Department's recruitment and retention efforts. A recent Congressional Budget Office report determined that federal workers with a bachelor's degree (one-third of the workforce) earned 10 percent less, on average, than their private sector counterparts, and federal workers with a professional or doctorate degree (one-tenth of the workforce) earned 29 percent less, on average, than similar workers in the private sector.

However, when the comparison is made using the total compensation package of federal employees, including all benefits, federal employees with a bachelor's degree averaged 5 percent more than their private sector counterparts. Compensation for professional or doctorate degree federal workers remained below that of the same group of private sector employees by 22 percent. While federal salaries may continue to lag behind those in the private sector, it is critically important that the Department recognize it can bridge the salary gap in the competition for highly qualified and diverse personnel by being attentive and responsive to work-life balance issues, such as workplace flexibilities, in formulating its human capital strategy.



Source: Congressional Budget Office

Managing Workplace Flexibilities

One of the challenges facing the Department in its effort to recruit top talent, while at the same time being attentive and responsive to work-life balance needs, is the issue of workplace flexibilities. In early 2024, the Department implemented a telework policy that requires employees to report to their office for in-person work at least 6 days per 2-week pay period. The updated telework policy allowed components to approve certain exceptions to this requirement, including to allow for remote work options. According to an Office of Management and Budget report issued in August 2024, Department employees spent 91.4 percent of regular working hours in person, and telework eligible employees spent 56.8 percent of regular working hours in person, excluding remote workers. Further, the report details the Department's plans to maintain operational readiness while promoting physical space efficiency, a resultant challenge as long-term decisions are made on flexible workplace policies.

The U.S. Office of Personnel Management's annual 2023 telework report stated that "telework can lead to greater operational resilience, increased productivity, higher employee engagement, lower employee attrition, expanded recruitment pools, and cost savings for both agencies and

employees," and concluded that employees who telework reported being less likely to leave their jobs. Similarly, a Congressional Budget Office report issued in April 2024 similarly found that flexibility to work from home has a positive effect on the ability of federal agencies to recruit and retain a highly qualified workforce.

Subsequently, four DOJ employee groups wrote to Deputy Attorney General Lisa Monaco and expressed concern about the potential impact on the DOJ workforce that could result from the more limited workplace flexibilities that DOJ components could offer to employees. The letter asked that DOJ enforce its in-person work policy (policy) equitably and assess its effects on the workforce. In response, the Department's Assistant Attorney General for Administration (AAG-A) wrote that the Department was: (1) monitoring hiring and retention data by demographics, (2) piloting an anonymous exit survey that would contain a question about in-person work, (3) working on regularly conducting a pulse survey that would include questions about the policy, and (4) working with component leadership to gauge the policy's effectiveness. Also, according to the AAG-A, Department leadership intends to review the 2024 Federal Employee Viewpoint Survey (FEVS) results, which contained questions about workplace flexibilities, to better understand workforce trends. The AAG-A stated that the Department would seek to understand the impact of its new in-person work policies on maximizing employee job satisfaction while maintaining efficient, effective, and economical operations.

Notwithstanding employee utilization of telework options and DOJ's operational need to understand the impact of these policies, the use of greater workplace flexibilities can also lead to significant rent cost savings for the Department. The August 2024 Office of Management and Budget report describes the Department's completed, in progress, and pending projects to reassess its footprint in the National Capital Region. For example:

- Over the past 5 years, the Federal Bureau of Investigation has consolidated 10 leases in the National Capital Region totaling approximately 502,000 square feet and $23.6 million in annual rent savings.

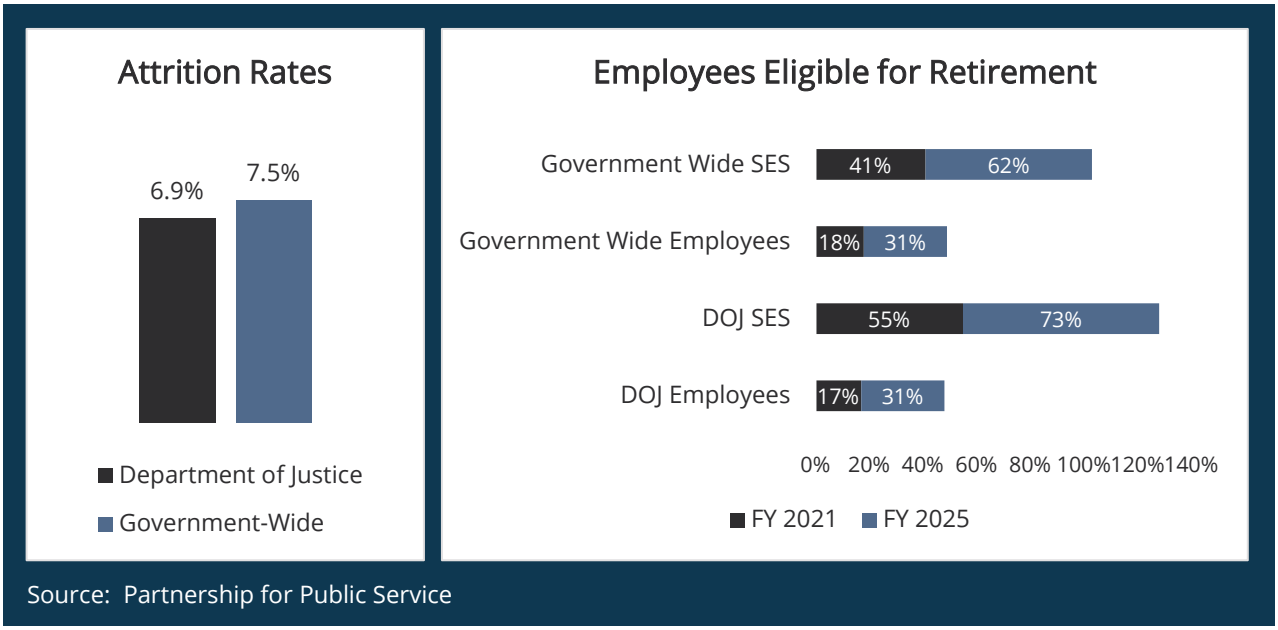
- Justice Management Division projects have reduced the Department's square footage by approximately 385,000 usable square feet and will produce an annual rent savings of approximately $25 million.

- The Office of Justice Programs will reduce its footprint by approximately 75,000 square feet this year.

- A pending consolidation proposal for the Department's 2 Constitution Square office space, housing Justice Management Division offices, will result in a further footprint reduction of 386,000 usable square feet.

Succession Planning and Knowledge Management

Emerging from the COVID-19 pandemic, succession planning and knowledge management are keys to building resilience in the DOJ workforce in order meet future demands. Key in doing so will be to implement strategies to attract and retain top talent, invest in training programs that equip employees with the skills and mindset to adapt to changing circumstances and maintain productivity with equitable access to secure technology in challenging environments. Current challenges the Department faces include the shifting generational make-up of the federal workforce, and how to manage a multigenerational workforce to meet the needs of Department employees without sweeping generalizations or biases.



Source: Partnership for Public Service

Succession planning allows agencies within the Department to preserve institutional knowledge and transfer experience to new employees with whom the Department has lost touch during the times of remote work. The Partnership for Public Service has not released new figures for the Department since 2022 but did identify a projected increase in attrition for 2025 of 31 percent for agency employees, and 73 percent for Senior Executive Service employees. This marked level of potential attrition of Senior Executive Service staff across the Department has the potential to degrade the management and mitigation of challenges the Department may soon face.

In 2021, the GAO published a report of their High Risk Series–Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas. A top area identified as requiring significant attention was strategic human capital management. Key drivers of attrition are limited opportunities for advancement, professional development, and retirement. Attrition has resulted in a loss of institutional knowledge, subject matter expertise, and gaps in leadership. The GAO notes leadership as the critical element for initiating and sustaining progress as leaders provide the needed support and accountability for managing risks.

Department Rankings Among Federal Agencies on Metrics Important to Employees

Over the past 10 years, the overall engagement and satisfaction score of the Department as reported by the Partnership for Public Service based on FEVS data has slipped from a ranking of 5 of 19 large agencies in 2013 to 16 out of 17 in 2023. Many of the Department's components have fared far worse during that same time period, with the Federal Bureau of Prisons dropping from a ranking of 148 out of 300 in 2013, to a ranking of 459 out of 459 in 2023. Similarly, the Department's Executive Office for Immigration Review fell from a ranking of 190 out of 300 in 2013 to 427 out of 459 in 2023.

The biggest swing, however, can be seen with the Federal Bureau of Investigation, which was ranked 73 out of 300 in 2013, but 412 out of 459 in 2023. The remaining large investigative agencies with the Department—Bureau of Alcohol, Tobacco, Firearms and Explosives; Drug Enforcement Administration; and U.S. Marshals Service—also experienced a downward trend in rankings of overall engagement and satisfaction as reported over the past 10 years. Recognizing, being responsive to, and appropriately addressing the shortfalls noted in the responses to overall engagement and satisfaction will be key to retaining staff and drawing new talent to the DOJ workforce.

The 2023 FEVS also introduced an Employee Experience index that measured employees' view of their workplace on factors such as feelings of accomplishment, attachment to one's work, and feelings of contributing to the common good. On that measure, DOJ ranked 4 percent lower than the whole government with a 69 percent index score compared to the government-wide index score of 73 percent. In view of the Department's inarguably compelling mission, such Department rankings appear to signal a need for the Department to carefully assess the reasons for these results and respond appropriately to them. Failure to do so is likely to have adverse consequences over time as those committed to public service opt to leave the Department for other agencies or the private sector and the Department seeks to recruit new personnel to replace them.

Additionally, as in previous years, the 2022-2026 DOJ Strategic Plan identified a diverse workforce as a key asset. To most effectively achieve its mission, the Department must continue to benefit from the broad and varied experiences and perspectives of its employees. To that end, the Department should continue to identify and implement best practices for recruiting, developing, and retaining highly qualified and diverse personnel. It will remain important for DOJ to continually evaluate recruitment strategies and assess trends in workplace demographic data to ensure it fully realizes the advantages that its greatest asset, the people who work at DOJ.

Workplace Harassment

Department leadership have made significant efforts to address sexual harassment in the workplace.

Source: Andrey Popov/stock.adobe.com

One of the significant challenges faced by the Department over the past decade has been the issue of harassment in the workplace. While the Office of the Inspector General continues to receive complaints from DOJ employees of sexual harassment in the workplace, as outlined in last year's Top Management and Performance Challenges report, Department leadership has made significant efforts to address the issue. In 2018, DOJ issued a memorandum for Heads of DOJ Components directing components to enforce the Department's zero-tolerance policy. In 2021, DOJ expanded its efforts through the issuance of a memorandum for all employees that established a steering committee to review the Department's sexual harassment policies. Furthermore, in 2023, DOJ appointed a director to oversee the Sexual Misconduct Response Unit which aims to: (1) issue a comprehensive Department-wide sexual misconduct policy, and (2) develop and implement new training across DOJ. The work of this new unit is ongoing.

As our Office of the Inspector General reports reflect, this issue remains a challenge for the Department, and it is therefore imperative that the Department continue to support these important steps and serve as a leader in maintaining a workplace free of sexual harassment and misconduct.

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

CONSOLIDATED MANAGEMENT RESPONSE TO THE OFFICE OF THE INSPECTOR GENERAL 2024 REPORT ON TOP MANAGEMENT AND PERFORMANCE CHALLENGES FACING THE DEPARTMENT OF JUSTICE

The Justice Department's mission is to uphold the rule of law, keep our country safe, and protect civil rights. In July 2022, the Justice Department (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. The 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, the OIG identified seven challenges it believes represent the most pressing concerns for the Department:

1. The Ongoing Crisis Facing the Federal Corrections System
2. Strengthening Public Trust in the U.S. Department of Justice
3. Promoting and Safeguarding National Security
4. Cybersecurity and Emerging Technology
5. Pursuing the U.S. Department of Justice's Law Enforcement Mission While Protecting Civil Rights and Civil Liberties
6. Strengthening the Administration and Oversight of Contracts and Grants
7. 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. The Ongoing Crisis Facing the Federal Corrections System

In its report, the OIG has pointed to the critical need for the Federal Corrections System to address staffing shortages in key positions, lack of sufficient funding to repair its crumbling infrastructure, and the introduction of contraband at its prisons.

The Department, including the Federal Bureau of Prisons (BOP), agrees. BOP has a dual mission – to foster a humane and secure environment and to ensure public safety by preparing individuals for successful reentry. It is obvious that widespread staffing shortages, crumbling infrastructure, and the presence of contraband are fundamental barriers to fulfilling this dual mission.

BOP has made progress tackling these considerable challenges, but it cannot do it alone. Addressing the staffing and infrastructure issues that the OIG identified will require transformational and long-overdue investment in the Federal Corrections System. For this reason, the Department has provided to Congress, with the support of the Administration, a funding proposal to address critical safety needs across the Federal Prison System. This plan lays out the funding necessary for BOP to:

- Hire much needed staff at more competitive salary levels,
- Reduce its need to engage in the counterproductive use of augmentation – a practice that hinders BOP's ability to implement the First Step Act, and
- Make critical, safety-related repairs to infrastructure.

The case for additional BOP funding is clear. The OIG, the Government Accountability Office (GAO), and Congress have all recognized the urgent need for action. Indeed, the OIG itself in numerous reports has highlighted the funding and resource needs of BOP. In 2023, GAO cited staffing challenges when adding Strengthening Management of the Federal Prison System to its High-Risk List. Congressional consensus for improving BOP facilities, programming, and safety is clear from this summer's nearly unanimous passage of the Federal Prison Oversight Act.

Without needed and essential funding, and despite the Department's focused and dedicated efforts to mitigate the problems facing BOP, the Department will be unable to solve the critical challenges outlined by the OIG.

Addressing staffing challenges. Hiring and retaining employees is critical for BOP to support both the well-being of its dedicated employees and the safety of those in BOP's care. BOP has implemented several strategies to address its staffing shortages, with demonstrable success.

- **Direct hire authority:** BOP worked with Office of Personnel Management (OPM) to put in place nationwide direct hire authority for Corrections Officers.
- **Data driven staffing:** BOP has also deployed, as of October 2024, an automated staffing tool that brings a data-driven decisionmaking capability to how it approaches staffing for all institution positions. This tool is new and will continue to improve.

However, BOP has taken measures to validate its performance to date and stands ready to discuss with OIG the substantial merits to its approach.

- **Employee Wellness Branch**: BOP is creating an Employee Wellness Branch dedicated to a nationwide approach to enhancing the wellbeing of our corrections professionals.

BOP has increased the number of new hires each of the past three years. Over that same period, BOP has reduced the number of departing employees each year. BOP's average time to hire for corrections officers is now 69 days – below the OPM standard of 80 days.

While BOP has become much more effective at recruiting, hiring, and retaining its staff, much work remains to be done. BOP offers some of the lowest salaries of any law enforcement entity – often dramatically lower than its state-level counterparts. For example, the New York City Department of Corrections advertised that an NYC corrections officer earned an average of $130,000 after three years. That same officer with the same tenure at BOP would earn only $114,000, and only after receiving a 35% retention incentive. With similar salary gaps throughout its system, it is obvious why BOP has struggled to address its staffing shortages.

To address these issues, the Department, on behalf of BOP, requested approval from the OPM for special salary rates to increase the base pay for corrections officers and certain medical staff. The Department is actively working with OPM so we can have the authority to increase base pay. If approved by OPM, these increased salaries could be available as soon as January 2025, subject to the availability of funding. There is every reason to believe increased salary through special salary rates would have a positive ability on BOP's ability to recruit and retain staff that would ameliorate the staffing challenges identified by OIG.

Repairing critical infrastructure. BOP maintains over 46,000 acres of land with more than 3,600 buildings that make up its over 120 institutions. Each of these institution needs repair - many critically so. If BOP cannot keep its roofs patched, fences maintained, facilities mold-free, HVAC operating, fire suppression systems active, and electricity on, FBOP cannot provide humane and secure facilities.

To address these critical infrastructure needs, BOP has worked with the Office of Management and Budget (OMB) to develop a Five-Year Infrastructure Strategic Plan. This longitudinal funding plan is structured to ensure that all critical needs are systematically addressed. This approach not only addresses immediate repair needs but also helps in planning for future maintenance, thereby promoting the long-term sustainability and functionality of the facilities. In addition to this plan, BOP continues to analyze its infrastructure requirements and develop methodologies that will provide additional funding priorities for critical requirements over the long term.

The FY 2024 enacted budget provided BOP with just $179.8 million, of which $147.8 million was available for addressing a crumbling infrastructure. The current backlog of unfunded critical needs totals over $3 billion. Absent a major investment in addressing these needs, BOP will be forced to continue triaging while the repair backlog further grows.

Disrupting the flow of contraband. Reducing, and ultimately ending pipelines for contraband is a top priority for BOP. BOP uses various methods to detect, identify, and disrupt the introduction of contraband, including requiring background checks for people coming inside BOP facilities, as well as using walk-thru metal detectors, drug screening machines, and whole-body imaging devices. BOP's Intelligence & Counter Terrorism Branch gathers intelligence and works with federal, state, and local law enforcement partners to disrupt large criminal operations, like drug cartels. BOP also partners with entities like the Federal Aviation Administration to use cutting edge technology to detect, and intercept contraband introduction via the use of Unmanned Aircraft Systems (UAS aka "drones").

BOP is taking several other steps to combat the flow of contraband:

- **Cameras upgrades**: BOP is implementing recommendations from with three OIG reports related to upgrading security cameras. BOP has installed fiber optics in over 71 percent of facilities, and those facilities are in the process of installing digital cameras. The remaining facilities are in the process of completing fiber optic installation. Once that is complete, work on the camera installation can begin.
- **Implementing new mail scanning procedures**: Illicit substances sent to incarcerated individuals through U.S. mail is a persistent and evolving challenge. To address this, BOP is putting into place new requirements for mail handling that will help combat contraband and improve the safety of our employees.
- **Expanding naloxone availability**: Because of the threat posed by contraband opioids, BOP is taking proactive steps to protect employees and incarcerated individuals in instances of opioid overdoses. Starting no later than November 4, 2024, all institutions will implement a NARCAN Self-Carry policy. NARCAN (naloxone) is an opioid overdose reversal medication that can save lives when administered quickly and effectively. BOP will purchase 100,000 doses of NARCAN that will be distributed to institutions in FY 2025.

Funding plan to address critical safety needs in the Federal Correctional System. The Department, including BOP, agrees with the OIG about the urgent need to address the challenges faced by the Federal Corrections System. BOP has and will continue to take steps within its existing authorities and resources to address these longstanding issues. The reality, however, is that BOP will need committed investment to address the root causes of its challenges. Put simply, BOP cannot hire more staff and offer them more competitive salaries if it does not have the funding. BOP cannot patch roofs or address other repairs to critical life-safety infrastructure if it cannot pay for repairs.

To this end, the Department developed a funding plan to transform the Federal Correctional System. This plan sets out, year-by-year, the resources that BOP needs to address the core issues raised by the OIG – a total of $4.4 billion of necessary investments in staffing and repairs. The Department has shared this information with Congress and stands ready to work with them to address this priority issue.

II. 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.

Building trust in law enforcement. The Department recognizes we cannot fulfill our mission as a law enforcement agency without the trust of the public we serve. We also know that the work of law enforcement professionals is essential. The work that these professionals do daily is extraordinarily difficult and often very dangerous, and their responsibilities are enormous. They are asked to keep their communities safe, to uphold the rule of law, and to ensure equal justice under law. We are committed to working with our partners in communities and police departments across the country to advance the accountability, transparency, and public trust that are essential to public safety.

Over the past year, the Department has worked diligently on more than 90 deliverables consistent with Executive Order 14074, *Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety* and engaged with stakeholders from civil rights, law enforcement, and community groups, as well as our federal agency partners. This work includes:

- Launching the National Law Enforcement Accountability Database (NLEAD) on December 18, 2023. NLEAD is a centralized repository for information documenting instances of federal law enforcement officer misconduct.
- Prohibiting the transfer or purchase of military-style weapons and equipment to state, tribal, local, and territorial (STLT) law enforcement agencies.
- Awarding grants in a manner that supports and promotes accountability. Starting with the FY23 grant cycle, in relevant solicitations, the Department included language outlining priority consideration for applicants who have policies or practices in line with certain substantive provisions of Executive Order 14074.
- Creating accreditation standards to help encourage STLT law enforcement agencies to adopt policies consistent with Executive Order 14074. These standards follow best policing practices in in areas such as: hiring and performance evaluation, use of force policies; use of in-car and body-worn cameras; and submission of important crime data to the Federal Bureau of Investigation (FBI).
- Promulgating an interim policy for facial recognition technology by the Department.

The Department has also created, as of December 2023, an Emerging Technology Board which includes representatives of all law enforcement components, to coordinate and govern AI and other emerging technology issues across the Department.

Building trust in the correctional system. The Department also recognizes its fundamental obligation to provide facilities that are safe for all 144,805 individuals in BOP custody and provide for the rehabilitation, health, and safety of incarcerated individuals; a safe and secure work environment for correctional professionals; and transparency and accountability across federal detention facilities.

The Department, including BOP, has made it a priority to address employee misconduct. BOP has significantly increased staffing levels in its Office of Internal Affairs (OIA) and Office of General Counsel (OGC). BOP expanded OIA by 119 positions and OGC by 14 new positions. It also reorganized OIA so its Special Investigative Agents (SIAs) now report centrally to BOP Headquarters as opposed to local wardens. These efforts have helped reduce the backlog of pending investigations and enhanced the effectiveness of SIAs. As OIA decreases processing time and the investigative backlog, investigation timelines improve, which reinforces accountability for misconduct – to the benefit of both employees and adults-in-custody.

Building trust through our internal accountability systems. The Department also remains steadfast in its commitment to ensuring that attorneys maintain the highest ethical standards to foster accountability and public trust. For over 49 years, the Department's Office of Professional Responsibility's (OPR) primary mission is 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. OPR maintains an effective system for investigating attorney professional misconduct and conducts its work independently. As a result of this independence, OPR's investigations are not influenced by any relationship with prosecutorial offices or the attorneys whose conduct OPR investigates, therefore giving the public reassurance that the commitment to strict adherence to Department policies, rules, and regulations is unwavering.

Regarding investigations of misconduct continuing post-separation, the FBI continues to work closely with the OIG to finalize policy regarding the continuation of investigations post separation. Today, all investigations involving FBI employees, regardless of the alleged violation, undergo careful review to determine whether the investigation should continue even if an employee separates under inquiry.

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 terrorism and 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.

Terrorism threats. As the FBI Director testified in December 2023, "[t]he greatest terrorism threat to our homeland is posed by lone actors or small cells of individuals who typically radicalize to violence online, and who primarily use easily accessible weapons to attack soft targets." The OIG report references its current review of the role and activity of the Department and its components in preparing for and responding to the events at the U.S. Capitol on January 6, 2021. The Department welcomes the OIG's review.

Election security. The Department maintains robust coordination between its relevant components – including the Criminal Division, the National Security Division, and the FBI – to ensure visibility into and deconfliction of investigations regarding foreign malign influence threats to our elections across components and to ensure that all Department actions are consistent with the Department's Election Year Sensitivities Policy. The Department, per these efforts, has recently charged and prosecuted multiple cases involving illicit foreign influence.

The FBI's core principles are grounded in protecting Americans' First Amendment right to free speech. Since at least 2019, the FBI operated under a set of principles related to interactions with social media companies and had policies in place specific to sharing foreign malign actor threat information with social media companies and to guide communications with third parties. These principles and policies were further supplemented with a robust set of standard operating procedures (SOPs) related to information sharing with social media companies in February 2024. Moreover, the FBI's investigative activities must comply with Attorney General Guidelines on Domestic Investigations (AGG-DOM) and the Domestic Investigations and Operations Guidance (DIOG). The FBI also adheres to a classified document formulated by the interagency which establishes principles and guidelines by which intelligence community members can analyze social media-related data in a manner that comports with constitutional protections. These three documents were all in effect as of October 2019, well before the development of the SOPs implemented in February 2024.

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. In this complex landscape, the Department plays both offense and defense – it must: protect its own systems from attack, effectively pursue malicious cyber actors, continuously modernize its own workforce, and adopt new technologies in responsible ways.

Enhancing cybersecurity defenses. To fulfill its mission, it is critical that the Department build and maintain robust cybersecurity defenses. This is critical for keeping our workforce productive while also safeguarding sensitive data.

To that end, the Department has made significant strides. The Department currently has the highest total score among CFO Act agencies based on the Office of Management and Budget's (OMB) and the Cybersecurity and Infrastructure Security Agency's cybersecurity metrics – known otherwise as the Federal Information Security Modernization Act (FISMA) scores. The Department is making progress on the recruitment and retention of cyber talent: it has implemented a pilot IT Cyber Retention Incentive Program that has shown positive results, and this retention incentive program will be made available more broadly across the Department in FY 2025.

The Department has made significant progress in mitigating supply chain risks. The Department's cyber supply chain risk management (C-SCRM) program – in which we have made concerted investments - has increased its company threat assessments for DOJ software and hardware in FY 2024. In addition, the Department has updated its existing guidance to ensure secure procurement, deployment, and implementation of Information Technology (IT) software, hardware, and services.

While the Department has come far, the critical importance of cybersecurity to our national security means that we cannot become complacent or move backwards. Inconsistent funding, however, jeopardizes this progress. The Department funds its cybersecurity infrastructure through the Justice Information Sharing Technology (JIST) appropriation. In FY 2024, this appropriation fell to $30 million. This is 1/5th of the amount this fund was appropriated in FY 2023. After adjusting for inflation, the fund is now at the lowest level in its history. The current successes in the Department's cybersecurity program reflects what can be achieved because of funding from FY 2023. Another year under similarly minimal funding levels to FY 2024 will erode the Department's ability to meet cybersecurity needs and fend off new and evolving attacks from malign actors and nation states.

Modernizing its workforce and adopting new technology in responsible ways. To evolve and keep pace with an evolving landscape, the Department must be able to attract and retain a highly skilled cyber workforce. The Department designated its first ever Chief Science and Technology Advisor and Chief Artificial Intelligence Officer in February 2024. This was an important step, but the Department must continue to build out a highly skilled cyber workforce. To do so, the Department will need hiring and salary authorities necessary to attract and retain

qualified candidates. The Department's current authorities limit options for bringing in talent and, most critically, leave the Department's salaries for cyber workers far out of step with other employers, including other federal agencies. Other agencies that are central to public safety and national security have been granted special cyber workforce authorities - the Department urgently needs a similar solution.

New and emerging technologies offer important opportunities to make the Department more effective and efficient upholding the rule of law, keeping the nation safe, and protecting civil rights. It also presents risks for misuse. The Department therefore formed an Emerging Technology Board that brings together the Justice Department's law enforcement and civil rights teams, along with other experts. The Department has charged this board with advising Department leadership on responsible and ethical uses of AI by the Justice Department. The Department also launched the Justice AI Initiative earlier this year, to inform the Justice Department's AI policy. Justice AI brings together stakeholders across civil society, industry, academia, and law enforcement to share outside expertise and a wide range of perspectives on both the promise of AI and the perils of its misuse.

V. Pursuing the Department'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 articulates 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." To promote public trust between communities and law enforcement, the Department supports efforts to make communities and policing safer while protecting individual civil rights and strengthening connections between law enforcement and the communities we serve.

Tackling violent crime. Core to the Department is its fundamental mission to keep the American people safe. In May 2021, the Department adopted a 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. Preliminary data from 88 cities showed that violent crime has continued to decline considerably in 2024, including a 16.9% decline in murder, a 7.5% decrease in rape, a 3.4% decrease in aggravated assault, and a 5.2% decline in robbery. Examples of the Department's efforts under its violent crime strategy include:

- The Criminal Division's Violent Crime Initiative, where Criminal Division prosecutors and Assistant U.S. Attorneys have surged enforcement and community outreach efforts and used data to focus on the most prolific offenders and recidivists responsible for violence. This initiative has included efforts in Houston, Hartford, Jackson, St. Louis, and Memphis.
- The Bureau of Alcohol, Tobacco, and Firearm's expansion of Crime Gun Intelligence Centers, which use cutting-edge technology to rapidly develop and pursue investigative leads, by analyzing firearm and ballistics evidence.
- Efforts by US Attorney's Offices across the country to crack down on violent crime during summer months, when violent crime historically surges. These efforts include: increased outreach and intervention activities, weekly data-driven coordination with local law enforcement to identify shooters and other drivers of violent crime for federal prosecution, surges in federal firearms prosecutions, increased focus on prosecution for possession or use of machinegun conversion devices, and carjacking task forces.
- The Drug Enforcement Administration's (DEA) Operation Overdrive, which uses a data-driven, intelligence-led approach to identify and dismantle criminal drug networks operating in areas with the highest rates of violence and overdoses.
- The U.S. Marshals Service's Operation North Star, which targeted fugitives and violent offenders in 10 metropolitan areas, prioritizing those who used firearms in the commission of crimes or signaled high risk factors for violence. Over 74 operational days in FY 2024, the U.S. Marshals Service arrested 3,421 violent fugitives, including 216 for homicide, 803 for assault, and 482 for weapons offenses in cities that included Dallas and Fort Worth, Texas; Charleston and North Charleston, South Carolina; Baton Rouge, Louisiana; Little Rock, Arkansas; Phoenix; St. Louis (to

include East St. Louis, Illinois); Birmingham, Alabama; Winston-Salem, North Carolina; Dayton, Ohio; and San Antonio.

Reducing the illegal use of opioids, including fentanyl. The Department is also committed to combatting the scourge of synthetic opioids like fentanyl. Over the past several years, the Department has focused marshalled and coordinated resources both within the Department and with other federal agencies, state and local law enforcement partners, and foreign government. This effort is aimed at breaking apart every link in the global fentanyl supply chain – from China to Mexico to the United States. This includes:

- Arresting and prosecuting cartel leaders, members, and associations – including charging and arresting the alleged leaders of the Sinaloa Cartel;
- Disrupting the chemical precursor supply chain – including charging China-based companies and their employees for crimes related to fentanyl and methamphetamine production, distribution of synthetic opioids, and sales resulting from precursor chemicals;
- Countering the fatal impacts of fentanyl – including expanding the "One Pill Can Kill" awareness campaign to include a partnership with the NFL Alumni Health Association and launching a One Pill Can Kill Game Over Sports Tournament designed to reach hard-to-reach younger demographics through an esports digital platform;
- Targeting criminal enterprises on the Darknet; and
- Building partnerships to combat transnational organized crime – including combatting the availability of illegal pill presses.

In 2024 to date, the DEA has seized over 47.7 million fentanyl pills and 5.8 thousand pounds of fentanyl powder. These seizures equate to over 292 million doses. The Department is also actively carrying out the directives of National Security Memorandum 24 – which drives information-sharing and coordination across the Executive Branch to counter fentanyl.

As noted by the OIG, the GAO issued a priority recommendation that the DEA solicit input from licensed distributors of controlled substances and develop additional guidance regarding their roles and responsibilities for monitoring and reporting suspicious prescription drug orders. The Department agrees that seeking such input would strengthen DEA guidance, improve communication with distributors, support the diversion mission, and ensure an adequate and continuous supply of controlled substances for legitimate medical needs.

Enforcing civil rights laws. Protecting civil rights is the Department's urgent charge today, as it was when the Justice Department was first established in 1870 with the first principal purpose of protecting the rights guaranteed by the 13th, 14th, and 15th Amendments. The Department has continued to advance the critical work of protecting voting rights, combatting hate crimes, fostering trust and accountability in law enforcement, expanding access to justice, improving the criminal justice system, protecting reproductive freedoms provided under federal law, advancing environmental justice, and tackling the climate crisis.

Moreover, 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.

Ensuring law enforcement accountability. The Department agrees with the OIG about the critical importance of law enforcement accountability. No law enforcement agency - including the Justice Department - can effectively do its work without the trust of the public. As noted by the OIG, DOJ launched the NLEAD earlier this year - an important new tool for our law enforcement agencies to vet and hire officers and agents. This database will make policing safer and more effective by strengthening trust between law enforcement officers and the communities they serve. But it will only do so if it receives the requisite support. The Department's FY 2025 President's Budget includes a request for $10 million and 2 positions to support this critical new resource.

Protecting vulnerable communities from abuse and exploitation. The Department takes as a core responsibility the need to protect the most vulnerable among our citizens, including children.

In response to OIG's 2024 report and recommendations on the FBI's handling of tips of hands-on sex offenses against children and mandatory reporting of suspected child abuse, the FBI implemented a series of changes to improve its operations. These efforts include:

- Re-establishing a dedicated Section within the Criminal Investigative Division to provide greater program oversight and accountability over the Violent Crimes Against Children program.
- Requiring supervisors to conduct quarterly file reviews of all open investigations managed by their agents and reporting officers.
- Enhancing the FBI's file review system to ensure that referrals to law enforcement or child protective services, have occurred, and have been documented.
- Instituting mandatory annual trainings and specialized trainings for crimes against children and human trafficking investigators.

The Department recognizes the swiftly changing nature of the threat. Since 2020, crimes against children cases have significantly increased by over 25% and the FBI's efforts, resulting in over 8,000 arrests, are evidence to our commitment to protect victims and combat child exploitation. Budget support is necessary to address the rise in crime – the Department requested an enhancement in the 2024 budget to be able to increase the number of personnel assigned to the Crimes Against Children threat, but that request was unfulfilled. The President's Budget for FY 2025 includes enhancement requests for the Crimes Against Children and Human Trafficking Programs.

VI. Strengthening the Administration and Oversight of 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.

Acquisitions. To address matters of compliance and reinforce proper operational procurement procedures, the Department, through its Justice Management Division, established an Acquisition Compliance Taskforce (ACT) and issued an Acquisition Policy Notice (APN) on Acquisition Planning in FY 2024. The taskforce brings together operational and policy subject matter experts that identify opportunities to collaborate and share best practices in avoiding and remedying contracting compliance issues. They also proactively research, resolve, and prevent procurement issues identified by GAO and the OIG. The Department, again through its Justice Management Division, issued an APN agency-wide which defined a framework for the Department's uniform approach to establishing policies and procedures governing development of the acquisition strategy, to include forecasting requirements, developing the requirements document, conducting market research, engaging in category management activities, and drafting the written acquisition plan.

Grants. 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 has put in place several processes to strengthen its management of a large portfolio of grants. The Office of Justice Programs (OJP) has taken the following steps:

- It consistently exceeds its statutory requirements for conducting comprehensive monitoring. In FY 2024, OJP completed in-depth programmatic monitoring of over 1,000 grants totaling $2.8 billion – this is approximately 80 percent more than the amount required by law.
- In FY 2024, OJP's Office of the Chief Financial Officer (OCFO) provided financial monitoring for the Department's entire grants portfolio, including OJP, the Office on Violence Against Women (OVW), and the Office of Community Oriented Policing Services (COPS Office). This led to identifying more than $7 million in questioned costs.
- It conducts pre- and post-award risk assessments designed to identify and mitigate risk of mismanagement, fraud, or waste by funding recipients.
- It conducts financial and programmatic monitoring of all its state administering agencies on a risk-informed four-year rotation. The in-depth monitoring checklists include a significant number of questions focused on monitoring a prime recipient's management of subrecipient awards.
- With advancements in its data analytic capabilities, it now has access to real time performance metrics at the grant, grantee and program level which allows for more effective oversight as well to inform training and technical assistance efforts for internal staff and/or funding recipients.

- It provides numerous training opportunities to ensure that award recipients understand the administrative, financial, and programmatic requirements of their awards, including grant misuse and fraud awareness.
- It provides extensive technical assistance to its recipients to help address audit issues and establish adequate policies and procedures, particularly to small non-profit organizations and local and tribal agencies that may have limited administrative capacity.

Grant money must and should be used by recipients for allowable, supportable expenses. The Department's Grants Financial Guide makes clear that grant recipients must maintain accounting systems that tracks specific information and documentation to support all receipts and expenditures and obligations of Federal funds. OJP also provides training, technical assistance and periodic guidance regarding the recipient requirement for adequate supporting documentation, including routine reminder emails to recipients to highlight critical requirements like this. OJP also uses an established risk assessment process to identify those entities and awards with the highest risk indicators which may result in questioned costs.

Regarding the recommendations from OIG's audit of Comprehensive Opioid, Stimulant, and Substance Abuse Program, OJP has taken action to ensure that it assesses applications to ensure that they are responsive to the solicitation goals and objectives, demonstrate the ability to successfully carry out the activities of the award, and comply with applicable federal statutes, regulations, and executive orders. OJP has also updated its FY 2025 Notice of Funding Opportunity (NOFO) templates (previously referred to as solicitation templates) to clarify the types of risk factors considered during the application review process. OIG closed the first recommendation in July 2024 and OJP will be working with the OIG to close the second recommendation.

The Office on Violence Against Women (OVW) undertakes efforts similar to OJP's, such as pre- and post-award risk assessments, robust programmatic monitoring, and a variety of trainings to prevent financial management problems. OVW also works with OIG to train both new grantees and new staff of existing grantees on administrative, financial, and programmatic requirements of their awards, including grant misuse and fraud awareness. Starting in FY25, OVW, not OJP, will manage the financial monitoring portfolio for OVW awards. This will improve OVW's ability to catch problems early and resolve them quickly. It will also streamline OVW grant operations and allow OVW to provide more tailored support to OVW grant recipients, aligning closely with VAWA statutory requirements and OVW's grants management processes.

Crime Victims Fund. The Department, through its Office for Victims of Crime, has significantly strengthened its oversight of the Crime Victims Fund over the last decade. It prioritizes in-depth monitoring of these awards, reviews risk-indicator reports to proactively identify and resolve potential issues and assesses the adequacy of how state administering agencies (SAAs) monitor subrecipients. Of the over $5 billion that the OIG has audited since FY 2015, only 0.3% has resulted in questioned costs.

VII. 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.

Employee engagement and feedback. Recognizing the need for robust data and feedback from its more than 115,000 employees, the Department has made a concerted effort to increase FEVS participation and expand listening opportunities. This marks the third straight year where the Department has increased its participation rate in OPM's Federal Employee Viewpoint Survey. Likewise, the Department has now seen three straight years of increasing scores for OPM's employee engagement index, global satisfaction index, and DEIA index scores. The Department also instituted the first agency-wide employee pulse survey in October 2024, increasing the pathways whereby employees can make themselves heard.

Strategic workforce planning. The Department, through its Human Resources Modernization and Transformation Strategy, is focused on creating and implementing department-wide developmental programs to ensure the workforce is prepared to address their daily mission requirements and be ready to adapt quickly to emerging and new initiatives. This includes expanding its mentoring programs, developing and implementing an early career development program designed to enhance its current workforce and improve opportunities for growth; and to attract, develop, and retain a diverse, multi-disciplined skilled future workforce. The Department is also developing its first ever SES candidate development program, to increase workforce resiliency.

* * *

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.