U.S. Department of Justice
FY 2023 PERFORMANCE BUDGET

Office of the Inspector General

Congressional Justification

Contents

I. Overview (Office of the Inspector General)

A. Introduction

In Fiscal Year (FY) 2023, the President's budget request for the Department of Justice (DOJ) Office of the Inspector General (OIG) totals $145.8 million, which includes $10 million from the Crime Victims Fund (CVF) for oversight of CVF, 570 FTE, and 560 positions (146 agents and 39 attorneys) to investigate allegations of fraud, waste abuse, and misconduct by DOJ employees, contractors, and grantees and to promote economy and efficiency in Department operations. Additionally, the OIG is requesting $6 million in annual carryover authority.

B. Background

The OIG was statutorily established in the Department on April 14, 1989. The OIG is an independent entity within the Department that reports to both the Attorney General and Congress on issues that affect the Department's personnel or operations.

The OIG has jurisdiction over all complaints of misconduct against DOJ employees, including the Federal Bureau of Investigation (FBI); Drug Enforcement Administration (DEA); Federal Bureau of Prisons (BOP); U.S. Marshals Service (USMS); Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); U.S. Attorneys' Offices (USAO); Office of Justice Programs (OJP); and other Offices, Boards and Divisions (OBDs). The one exception is that allegations of misconduct by a Department attorney or law enforcement personnel that relate to the exercise of the Department attorneys' authority to investigate, litigate, or provide legal advice are the responsibility of the Department's Office of Professional Responsibility (OPR).

The OIG investigates alleged violations of criminal and civil law, regulations, and ethical standards arising from the conduct of Department employees in their numerous and diverse activities. The OIG also audits and inspects Department programs and assists management in promoting integrity, economy, efficiency, and efficacy. The Appendix contains a table that provides statistics on the most recent semiannual reporting period. These statistics highlight the OIG's ongoing efforts to conduct wide-ranging oversight of Department programs and operations.

C. OIG Organization

The OIG consists of the Immediate Office of the Inspector General and the following six divisions and one office:

Audit Division is responsible for independent audits of Department programs, computer systems, and financial statements. The Audit Division has regional offices in Atlanta, Chicago, Denver, Philadelphia, San Francisco, and Washington, D.C. Its Financial Statement Audit Office, Computer Security and Information Technology Audit Office, and Office of Data Analytics are located in Washington, D.C. Audit Headquarters consists of: the Immediate Office of the Assistant Inspector General for Audit, Office of Operations, and Office of Policy and Planning.

Investigations Division is responsible for investigating allegations of bribery, fraud, abuse, civil rights violations, and violations of other criminal laws and administrative procedures

governing Department employees, contractors, and grantees. The Investigations Division has field offices in Chicago, Dallas, Denver, Los Angeles, Miami, New York, and Washington, D.C. The Fraud Detection Office and the Cyber Investigations Office are located in Washington, D.C. The Investigations Division has smaller area offices in Atlanta, Boston, Trenton, Detroit, El Paso, Houston, San Francisco, and Tucson. Investigations Headquarters in Washington, D.C., consists of the Immediate Office of the Assistant Inspector General for Investigations and the following branches: Operations, Operations II, Investigative Support, Hotline Operations, and Administrative Support.

Evaluation and Inspections Division conducts program and management reviews that involve on-site inspection, statistical analysis, and other techniques to review Department programs and activities and makes recommendations for improvement.

Oversight and Review Division blends the skills of Attorneys, Investigators, Program Analysts, and Paralegals to review Department programs and investigate sensitive allegations involving Department employees and operations and manage the whistleblower program.

Information Technology Division executes the OIG's IT strategic vision and goals by directing technology and business process integration, network administration, implementation of computer hardware and software, cybersecurity, applications development, programming services, policy formulation, and other mission-support activities.

Management and Planning Division provides advice to OIG senior leadership on administrative and fiscal policy and assists OIG components in the areas of budget formulation and execution, security, personnel, training, travel, procurement, property management, telecommunications, records management, quality assurance, internal controls, and general support.

Office of the General Counsel provides legal advice to the OIG management and staff. It also drafts memoranda on issues of law; prepares administrative subpoenas; represents the OIG in personnel, contractual, ethics, and legal matters; and responds to Freedom of Information Act requests.

D. Notable Highlights, Reviews, and Recent Accomplishments

1. Strengthening Public Trust in the Department of Justice

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

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

Maintaining Independence from Political Influence by Adhering to and Strengthening Policies Designed to Ensure Objectivity and Impartiality
Numerous national events in the past year have crystalized the urgency for the Department to address this challenge in a meaningful way. Public reports that political considerations allegedly influenced the Department's decision to obtain communications of members of Congress and the media, accusations that lawful protestors were cleared from Lafayette Square for political purposes, as well as claims that some Department officials may have sought to take action to alter the outcome of the 2020 election have all raised questions about the Department's objectivity and impartiality.

Improving Public Trust Through Effective Law Enforcement, Adherence to Policies, Strong Interagency Coordination, and Vigorous Oversight
Enhancing trust is critical because a constructive relationship between the police and the communities they serve is essential to effective policing. Law enforcement failures, including those that violate civil rights, affect public safety, and undermine individuals' privacy rights, damage public trust and have lasting effect. Effective law enforcement, strong interagency coordination, careful adherence to policies governing sensitive investigative authorities, and vigorous oversight of law enforcement are important components of the Department's effort to maintain its integrity and the integrity of all law enforcement.

A Commitment to Transparency and Accountability Can Build Public Trust in the Department
Holding Department personnel accountable for their misconduct remains an essential element of strengthening the public's trust in DOJ. Accountability is particularly challenging in instances where the Department employee retires or resigns before allegations of misconduct can be fully

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

Examples of OIG Work:

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

In July 2021, an audit report was issued. The OIG found that FBI senior officials failed to respond to allegations of sexual abuse with the utmost seriousness and urgency that they deserved and required. Among the failures was a lack of expeditious notice to state and local law enforcement, or other FBI field offices with stronger jurisdictional links to the allegations, in order to mitigate the ongoing danger posed by Nassar. In a statement, the FBI acknowledged its actions and inactions were a "breach of trust." In light of these findings, the FBI advised the OIG that it has reviewed applicable policies, procedures, training, and programs, and is in the process of making changes to strengthen the FBI's handling of future sexual abuse allegations. The OIG's oversight will continue through its review of the FBI's implementation of the OIG's recommendations.

Review of the Department of Justice's Planning and Implementation of Its Zero Tolerance Policy and Its Coordination with the Departments of Homeland Security and Health and Human Services

In January 2021, a report was issued. The OIG found that senior DOJ officials failed to coordinate the policy with relevant U.S. Attorney's Offices, the U.S. Marshals Service, the U.S. Department of Health and Human Services, or the federal courts. The review found that the Department's single-minded focus on increasing immigration prosecutions came at the expense of careful and appropriate consideration of the impact that such prosecutions and resulting family separations would have on children and the government's ability to later reunite the children with their parents.

Audit of the Federal Bureau of Investigation's Execution of Its Woods Procedures for Applications Filed with the Foreign Intelligence Surveillance Court Relating to U.S. Persons

In September 2021, the OIG released an audit report that confirmed that problems with implementation of the FBI's factual accuracy review procedures ("Woods Procedures") were not isolated to the FISA applications examined in our Crossfire Hurricane review.
The OIG made 10 recommendations to the FBI and the National Security Division to strengthen the Woods Procedures and reduce the risk of erroneous information being included in FISA applications, which can lead to faulty probable cause determinations and the infringement of U.S. persons' civil liberties. At the time the report was published, the FBI and the National Security Division had taken sufficient action to close 5 of the 10 recommendations issued to them collectively.

Audit of the Department of Justice Policy on Body Worn Cameras

In June 2021 the OIG released a report on the Department of Justice Policy on Body Worn Cameras for Law Enforcement Officers. In the past decade, DOJ has studied, supported, and promoted the use of body worn cameras through its Office of Justice Programs, which has

provided over $115 million to state, local, and tribal law enforcement agencies to create or enhance their body worn cameras programs. However, the DOJ Office of the Inspector General (OIG) found that when our audit commenced in June 2020, the DOJ did not have a body worn camera program for DOJ law enforcement officers (LEOs) and the Bureau of Alcohol, Tobacco, Firearms, and Explosives; Drug Enforcement Administration; FBI; and U.S. Marshals Service (the Components) were generally unprepared to implement body worn camera programs.

Ongoing Work:

Audit of the Federal Bureau of Investigation Office of General Counsel's Roles and Responsibilities

The OIG is conducting an audit of the FBI Office of General Counsel's (OGC) roles and responsibilities. The preliminary objective is to review the roles and responsibilities of the FBI OGC in overseeing compliance with applicable laws, policies and procedures relating to the FBI's national security activities. This audit was requested by the Attorney General and as stated in his August 31, 2020 memorandum "Augmenting the Internal Compliance Functions of the Federal Bureau of Investigation."

Review of the Department of Justice's Use of Subpoenas and Other Legal Authorities to Obtain Communication Records of Members of Congress and Affiliated Persons, and the News Media

The DOJ OIG is reviewing the DOJ's use of subpoenas and other legal authorities to obtain communication records of Members of Congress and affiliated persons, and the news media in connection with recent investigations of alleged unauthorized disclosures of information to the media by government officials. The review will examine the Department's compliance with applicable DOJ policies and procedures, and whether any such uses, or the investigations, were based upon improper considerations. If circumstances warrant, the OIG will consider other issues that may arise during the review. The review will not substitute the OIG's judgment for the legal and investigative judgments made in the matters under OIG review.

Review Examining DOJ's and its Law Enforcement Components' Roles and Responsibilities in Responding to Protest Activity and Civil Unrest in Washington, DC and Portland, Oregon

The OIG initiated a review of the Department's roles and responsibilities in responding to protest activity and civil unrest on June 1, 2020, at Lafayette Square. The OIG will examine DOJ law enforcement personnel's compliance with applicable identification requirements, rules of engagement, and legal authorities. The review will also consider law enforcement personnel's adherence to DOJ policies regarding the use of less-lethal munitions, chemical agents, and other uses of force.

Report to Congress on Implementation of Section 1001 of the USA Patriot Act

Section 1001 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) directs the OIG to receive and review complaints of civil rights and civil liberty violations by DOJ employees, to publicize how people can contact the OIG to file a complaint, and to send a semiannual report to the Congress discussing the OIG's implementation of these responsibilities.

In February 2022, the OIG issued its most recent report summarizing the OIG's Section 1001 activities from July 1, 2021 through December 31, 2021. Between this period covered by this

report, the OIG processed 627 new complaints that were identified by the complainant as civil rights or civil liberties complaints.

Of these complaints, 592 did not fall within the OIG's jurisdiction or did not warrant further investigation. These complaints involved allegations against agencies or entities outside the DOJ, including other federal agencies, local governments, or private businesses, as well as allegations that were not suitable for investigation by the OIG, and could not be or were not referred to another agency for investigation, generally because the complaints failed to identify a subject or agency.

The OIG found that the remaining 35 of the 627 complaints it received involved DOJ employees or DOJ components and included allegations that required further review. The OIG determined that 33 of these complaints generally raised management issues unrelated to the OIG's Section 1001 duties and referred these complaints to DOJ components for appropriate handling. Examples of complaints in this category included allegations by federal prisoners about the general prison conditions, and by others that the FBI did not initiate an investigation into particular allegations.

The OIG identified 2 complaints warranting further investigation to determine whether Section 1001-related abuses occurred. The OIG referred one of the complaints to the BOP and the other to the FBI and requested a copy of the investigative reports upon completion of the BOP and FBI investigations.

2. The Department's Contingency Planning Post-Pandemic

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

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

Examples of OIG Work:

BOP's Preparedness and Response to the Pandemic

In March and April 2020, the OIG initiated 16 remote inspections of facilities housing BOP inmates, including 11 BOP-managed facilities, 3 contract prisons, and 2 Residential Reentry Centers (RRC). The objective of the inspections was to evaluate the response to the pandemic at each inspected location. Between July 2020 and March 2021, the OIG issued 15 reports providing the results of these inspections.

Review of the USMS's Response to the COVID-19 Pandemic

In February 2021, the OIG released a report examining the United States Marshals Service's (USMS) response to the COVID-19 pandemic. The OIG found that while the USMS has taken steps to prepare for, prevent, and manage the risks associated with COVID-19, opportunities for improvement remain. For example, the OIG found that the USMS's detention facility oversight plan was inconsistent and did not ensure that all active facilities were assessed for implementation of the latest Centers for Disease Control and Prevention (CDC) guidance. Facilities operated by the USMS's state and local government partners under Intergovernmental Agreements (IGA) did not receive the same scrutiny from the USMS as do the USMS contract facilities, although the IGA facilities house approximately 70% of the USMS's 61,000 detainees. Additionally, we found that the USMS had a practice of transporting detainees without first testing to confirm that they were COVID-19 free. We believe this practice may lead to further infections and should be re-evaluated. The OIG made six recommendations to assist the USMS in mitigating the health risks arising from the pandemic. The USMS agreed with all six recommendations.

Review of EOIR's Response to the COVID-19 Pandemic

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

Survey of DOJ Litigating Attorneys and Immigration Judges on Work Experiences during the COVID-19 Pandemic

The OIG surveyed DOJ litigating and adjudicating personnel to gain an understanding of the impact of the pandemic on the workforce, coordination efforts, and casework, as well as anticipated conditions for a post-pandemic work environment. This effort was achieved through the dissemination of two surveys between May and June 2021.

- **Pandemic Operating Environment.** Over 65% of attorneys responded that they have teleworked full-time during the pandemic with ad hoc trips into the office for mission-critical work. A majority of these attorneys reported that they received sufficient access to guidance, equipment, software, and personnel. By contrast, about 37% of immigration judges indicated that they have teleworked full-time. EOIR judges described being able to complete certain activities while teleworking like legal research and checking emails; however, many judges described frustration over the inability to hear cases while teleworking.
- **Workload Changes.** Over 95% of attorneys noted that their workload increased or stayed the same during the pandemic, and while 40% reported a negative effect to work-life balance, only 24% indicated a decrease in job satisfaction. Attorneys' comments reflected that while teleworking provided the benefit of eliminating their commute, it also resulted in increased stress, burn out, or unsustainable workloads. More than 57% of responding EOIR judges reported that their workload decreased, and they noted the changes in their workload resulted in enhanced work-life balance. However, the OIG received approximately 30 comments from judges expressing a general belief that there was an unfair division of labor between judges whose dockets were suspended during the pandemic and those who still had active dockets, and for judges who were granted accommodations allowing them to remain home.
- **Coordination**. In general, most attorneys noted a similar level of coordination with outside parties when compared to before the pandemic. In contrast, most EOIR judges felt that they were not able to maintain a similar level of interaction with many of the entities traditionally involved in their cases—such as individuals subject to immigration proceedings and DHS attorneys who represent the federal government in removal proceedings.
- **Expectations for the Post-Pandemic Operating Environment**. Both attorneys and EOIR judges noted that in the post-pandemic operating environment, they would like their components to expand the availability of telework and other workplace flexibilities that were either unavailable or not as readily available prior to the pandemic.

Ongoing Work:

Ongoing Oversight of Bureau of Prisons response to the pandemic

The OIG is conducting further oversight of the BOP's response to the pandemic and expects to issue additional products to assist the BOP with improving its planning and preparedness for emergency conditions. First, the OIG is working on a capstone report that will draw conclusions and make recommendations based on the OIG's findings from across the 15 published remote inspection reports. Second, while the OIG has released the results[1] of a follow-up survey it conducted in 2021 of BOP institution staff, the OIG is completing, and will be publishing, a survey of BOP inmates seeking their perspectives about the BOP's response to the pandemic. Third, the OIG is undertaking a review examining the BOP's use of home confinement as a tool to mitigate the effect of the COVID-19 pandemic on the federal prison population.

[1] https://experience.arcgis.com/experience/582f32f0127c4c86870b2e129c05b9bc

3. Maintaining a Safe, Secure, and Humane Prison System

The Federal Bureau of Prisons' (BOP) mission is to maintain a safe, secure, and humane prison system. The Coronavirus Disease 2019 (COVID-19) pandemic abruptly presented complexities to the BOP's ability to fulfill its mission, and the ongoing pandemic continues to challenge the BOP. Issues raised by the pandemic exacerbated, or diverted attention from, other longstanding challenges confronting the BOP, such as staffing shortages, contraband, inmate medical care costs, and infrastructure maintenance.

Institutional Infrastructure, Physical Safety, and Security
The BOP's mission includes providing safe, humane, cost-efficient, and appropriately secure housing for inmates in its custody. This mission comes with several challenges, including managing the aging infrastructure of 122 institutions as well as implementing new technologies to detect and prevent security risks from entering the institutions. The OIG continues to identify work deficiencies in the institutional infrastructure, physical safety, and security of BOP facilities.

Inmate Healthcare and Welfare
The BOP has long faced challenges with issues surrounding provision of healthcare to inmates in its custody. The most recent manifestation of this issue arose during the pandemic and starkly demonstrated the challenges that the BOP and the Department face. In the OIG's remote inspections of 16 BOP-managed, contract, and Residential Reentry Center facilities, the OIG reported that medical and correctional staffing shortages undermined the BOP's response to the pandemic and impaired its ability to provide adequate medical care to inmates.

Programs to Reduce Recidivism
Inmate programming is a necessary part of rehabilitation and preparation for reentry into society. That is particularly true for federal inmates because approximately 97 percent of them will reenter society at the end of their sentence. Consistent with that need, the BOP utilizes programs for education, reentry preparation, and religious needs, among others. BOP institutions continue to suffer from a lack of programming staff to sufficiently meet the inmates' needs.

Example of OIG Work:
Review and Inspection of Metropolitan Detention Center Brooklyn Facilities Issues and Related Impacts on Inmates
In a 2019 OIG inspection, we found that Metropolitan Detention Center (MDC) Brooklyn had long-standing unaddressed temperature regulation issues, causing temperatures to fluctuate above and below the BOP's target temperature throughout the facility. Although the BOP has taken some steps to address the infrastructure-related issues at MDC Brooklyn and system-wide that were identified in the report, seven of the nine recommendations remain open.

Management Advisory Memorandum: Notification of Security Concerns at the Federal Bureau of Prisons Camp Locations
In June 2021, the OIG issued a Management Advisory Memorandum to the BOP identifying multiple security concerns at BOP camp facilities, including nonfunctional alarms and a lack of video surveillance on exterior doors. The memorandum identified multiple security concerns at BOP camp facilities, including nonfunctional alarms and a lack of video surveillance on exterior doors.

Management Advisory Memorandum: Notification of Needed Upgrades to the Federal Bureau of Prisons' Security Camera System

Although the BOP has made some progress implementing camera upgrades, because of the critical nature of this ongoing concern, in October 2021, the OIG issued a Management Advisory Memorandum to BOP recommending that it identify enhancements needed to address camera functionality and coverage deficiencies, provide cost projections to fund the upgrades, and include an estimated timeline for completion of the work. The OIG recommended that BOP identify additional enhancements needed to address camera system functionality and coverage deficiencies, provide cost projections to fund the upgrades, and include an estimated timeline for completion of the work.

Management Advisory Memorandum: Notification of Urgent Security Concerns Involving Staff Entering BOP Facilities

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

Audit of the Department of Justice's Efforts to Protect Federal Bureau of Prisons Facilities Against Threats Posed by Unmanned Aircraft Systems

In September 2020, the OIG issued a report which contains seven recommendations to improve the BOP's tracking of drone incidents and promote efforts to protect its facilities against drone threats. The BOP and DOJ agreed with these recommendations and on April 13, 2020, the Attorney General finalized guidelines on how DOJ components will be authorized to counter drone threats.

Audit of the Federal Bureau of Prisons' Perimeter Security Strategy and Efforts Related to the Contract Awarded to DeTekion Security Systems, Incorporated, to Update the Lethal/Non-Lethal Fence at Nine United States Penitentiaries

In September 2020, OIG issued a report of an audit of the BOP's perimeter security strategy and efforts related to the award of a security-related contract, the OIG identified a need for the BOP to improve its guidelines related to perimeter security and ensure that deficiencies identified and addressed at one facility did not also exist at other similarly situated facilities.

Audit of the Federal Bureau of Prisons' Management and Oversight of its Chaplaincy Services Program

In a July 2021 audit of the BOP's management of its Chaplaincy Services Program the OIG found that the BOP lacked service providers to adequately provide services for the diverse faiths found in the inmate population. We reported that 30 percent of its 122 institutions lacked appropriate chaplaincy services staffing under BOP guidelines, and that a lack of faith diversity among the BOP's chaplaincy staff left some inmate faith groups significantly underrepresented. Moreover, while it is critical for the BOP to understand whether its programs are effective in reducing the rate of recidivism so it can modify them as necessary and expand those that are

most effective, the BOP has failed to publish a more recent recidivism study since its review of the residential drug treatment programs available to federal inmates in 2001.

Ongoing Work:

BOP's Efforts to Address Inmate Sexual Harassment and Sexual Assault against BOP Staff
As of March 2021, the OIG continues to conduct a review of the BOP's efforts to address inmate-on-staff sexual misconduct. The review will assess the prevalence and impacts of inmate-on-staff sexual misconduct, including sexual harassment, assault, and abuse, in BOP institutions from FY 2008 through FY 2018.

Audit of the Federal Bureau of Prisons' Efforts to Construct and Maintain Institutions
The OIG is conducting an audit of the BOP's efforts to construct and maintain institutions. The preliminary objectives are to evaluate BOP's: (1) expansion of existing institutions, as well as its acquisition and construction of new institutions; and (2) maintenance of existing institutions, including how BOP identifies and implements modernization and repair projects.

4. Countering Domestic and International Terrorism and Safeguarding National Security

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

The Department's Preparedness and Response to Domestic Threats
One of the most difficult aspects of combating acts of violence in furtherance of political and social goals is the fact that support for such acts can be closely connected to protected First Amendment speech or activity. Striking the balance between vigorously protecting the security of the nation without impinging upon freedom of expression and other civil liberties is particularly difficult in the context of these domestic threats. The OIG's oversight of DOJ's efforts to confront the threat of violent acts in furtherance of political and social goals is ongoing.

Counterintelligence and Espionage
The Department's strategic plan identifies hostile intelligence activities and espionage as one of the gravest threats to national security. In addition to foreign governments, hostile foreign actors include non-traditional collectors, foreign corporations, and transnational organized crime groups targeting non-government information. While the threats posed in this area are substantial, the challenge facing the Department and the FBI is that it also must be vigilant in ensuring that it follows policies and processes to ensure investigations are factually predicated and not based on ethnic profiling or other improper considerations. This challenge is exemplified in the OIG's 2019 review of certain aspects of the FBI's Crossfire Hurricane investigation.

Disrupting and Defeating Foreign Terrorist Operations
Foreign terrorist organizations (FTO) continue to threaten the national security interests of the United States. According to the U.S. Department of Homeland Security, FTOs such as Al-Qaeda and the Islamic State of Iraq and ash-Sham (ISIS) will maintain a high interest in carrying out

attacks within the United States. In disrupting and defeating FTOs, DOJ is likely to face many challenges ahead.

Combatting Insider Threat and Unauthorized Disclosures
DOJ also faces the challenge of continuing to position itself to detect, deter, and mitigate insider threat risks, which continue to present significant harm to the security of the United States. While insider threats and unauthorized disclosures present a serious challenge, the Department must also remain committed to upholding whistleblower rights and protections that allow for DOJ employees or DOJ-affiliated individuals to report wrongdoing in accordance with the laws and rules that govern the release of both unclassified and classified information.

Examples of OIG Work:

Management Advisory Memorandum: Notification of Insider Threat Risk at the Department of Justice and the Drug Enforcement Administration
The OIG issued a Management Advisory Memorandum in February 2021 after becoming aware that Drug Enforcement Administration (DEA) contractors were not obligated to annually renew their On-Site Contractor Responsibilities document, which prohibits contract employees from engaging in personal and business associations with persons known to be convicted felons or associated with criminal activity. The OIG found this information concerning, as contracting staff are capable of holding sensitive, classified information. The DEA took corrective action and the two recommendations directed towards the DEA were closed in September 2021.

Audit of the Federal Bureau of Investigation's Efforts to Identify Homegrown Violent Extremists through Counterterrorism Assessments
In March 2020, the OIG issue a report of the FBI's efforts to identify HVEs through counterterrorism assessments. The audit found that the FBI had not taken a comprehensive approach to resolving deficiencies in its counterterrorism assessment process. Following attacks conducted by individuals who had previously been assessed or investigated by the FBI, the FBI conducted reviews to evaluate its process for assessing potential HVEs, yet the Office of the Inspector General (OIG) found that the FBI had not fully implemented the recommendations that emerged from these prior reviews. Subsequently, the FBI conducted another review to evaluate the investigative thoroughness of closed counterterrorism assessments. While the FBI determined that 6 percent of the closed assessments did not adequately assess the potential threat, the OIG found that nearly 40 percent of those assessments went unaddressed for 18 months after the deficiencies were known to the FBI. The OIG also identified inconsistencies in the FBI's reevaluation of closed counterterrorism assessments, as well as emerging challenges that the FBI must address when assessing potential HVEs. The audit resulted in seven OIG recommendations that aim to assist the FBI in its efforts to identify HVEs through counterterrorism assessments.

Audit of the Department of Justice's Strategy to Address the Domestic Violent Extremist Threat
In September 2021, the OIG issued an audit report reviewing the Department's strategy to address the DVE threat. The preliminary objectives of the audit are to: (1) evaluate the Department's efforts to develop a comprehensive strategy to address the DVE threat in the United States, and (2) determine if the Department is effectively coordinating among Department stakeholders on the implementation of its strategy. This audit will focus on Department-level efforts to coordinate an effective approach to identify, investigate, and prosecute DVE threats and promote information-sharing among Department components, as well as with the Department's federal, state, and local partners.

Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation

In December 2019, the OIG released this review which demonstrated the importance of safeguarding our country's civil rights and liberties while countering the threats posed by hostile intelligence activities and espionage. Since the release of this report, the FBI has agreed with the report's findings and has already demonstrated its commitment to remedial action by implementing several new initiatives, including evaluating its Foreign Intelligence Surveillance Act (FISA) application and renewal processes and requiring training for employees who handle FISA matters. The OIG will continue to monitor these and other measures taken by DOJ and the FBI to ensure that each of the nine recommendations the OIG made in its review is fully implemented.

Audit of the Federal Bureau of Prisons' Monitoring of Inmate Communications to Prevent Radicalization

In March 2020, the OIG completed an audit of the BOP's monitoring of inmate communications to prevent radicalization, which found significant weaknesses in the designation and monitoring of inmates with a known nexus to domestic or international terrorist organizations. The OIG provided the BOP with 17 recommendations, including eliminating the automatic delivery of email to high-risk inmates, determining and maintaining an accurate count of international and domestic terrorists incarcerated at, or in transit to BOP facilities, and improving audio equipment in BOP visiting rooms utilized by terrorist inmates subject to Special Administrative Measure directives. As of September 2021, 13 of the 17 recommendations from this audit remain open.

Audit of the Federal Bureau of Prisons' Management and Oversight of its Chaplaincy Services Program

In July 2021, the OIG completed a report on the BOP Management and Oversight of its Chaplaincy Services Program, which found significant deficiencies in the BOP's ability to prevent inmate access to prohibited content that advocated violence and religious extremism. The OIG also found that the BOP's internal policies do not restrict certain inmates from leading religious services and appear to be inconsistent regarding the level of required monitoring. For example, the OIG found that some institutions permitted inmates with a known nexus to international or domestic terrorism to lead religious services thereby creating a risk that, without clear policy and consistent monitoring efforts, these high-risk inmates could use their religious leadership roles to engage in prohibited activities or as a method to obtain power and influence among the inmate population. The OIG made five recommendations to the BOP to improve the delivery of religious services to the inmate population and to help diversify and alleviate shortages in its chaplain staff.

Ongoing Work:

Review examining U.S. Capitol events on January 6, 2021

This review will examine information concerning the January 6 events that was available to DOJ in advance of January 6; the extent to which such information was shared by DOJ with the U.S. Capitol Police and other federal, state, and local agencies; and the role of DOJ personnel in responding to this event. The OIG's review will also assess whether there are any weaknesses in DOJ protocols, policies, or procedures that adversely affected the ability of the Department to effectively prepare for and respond to the events at the U.S. Capitol. The OIG is mindful of the sensitive nature of the ongoing criminal investigations and prosecutions related to the events of

January 6. Consistent with long-standing OIG practice, in conducting this review, the OIG will take care to ensure that the review does not interfere with these investigations or prosecutions.

Review examining events at Lafayette Square on June 1, 2020
The OIG has initiated a review to examine DOJ's roles and responsibilities in responding to protest activity and civil unrest at Lafayette Square on June 1, 2020. This review will examine the training and instruction that was provided to DOJ law enforcement personnel; compliance with applicable identification requirements, rules of engagement, and legal authorities; and adherence to DOJ policies regarding the use of less-lethal munitions, chemical agents, and other uses of force.

5. Protecting the Nation and Department against Cyber-Related Threats and Emerging Technologies

Cyber breaches and attacks represent a growing threat to individual privacy, economic interests, and national security and is one of the most significant challenges facing the Department. As outlined in Executive Order (EO) 14028[2], Improving the Nation's Cybersecurity, the "United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy." As a member of the law enforcement and intelligence community, and as the holder of sensitive and classified information, the Department has a significant responsibility to combat threats such as cyber supply chain attacks and ransomware and to investigate and prosecute cybercrime. Other facets of the cyber-related challenges facing DOJ are safeguarding sensitive and classified data and strengthening its information technology (IT) systems.

Threat of a Cyber Supply Chain Attack and Threat Ransomware
Cyber supply chain attacks are a significant concern to the Department. Another threat to the Department, as noted by Deputy Attorney General Lisa Monaco in her remarks on June 7, 2021, are ransomware attacks, which have increased in both scope and sophistication in the last year and pose a threat to U.S. national and economic security.

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

Partnerships
Another challenge that the Department faces in investigating cyber threats is forming partnerships with private sector entities, state and local law enforcement, other federal agencies, and international law enforcement counterparts, including the International Criminal Police Organization (INTERPOL). With an increase in cybercrime and the growing complexity and international nature of such activity, it is important for DOJ to continue to maintain and develop further robust partnerships worldwide.

Strengthening the Department's Cyber Capabilities and Defenses

[2] https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf

The Federal Information Security Modernization Act (FISMA) requires each federal agency to develop and implement an agency-wide information security program. Throughout FY 2020, as required by FISMA, the OIG continued to assess the effectiveness of DOJ's information security program and practices. Majority of the FY 2020 FISMA audits led to at least one recommendation designed to strengthen component-specific information systems.

The onset of the Covid-19 pandemic presented the Department with an unexpected challenge, as the number of its employees working remotely increased exponentially. The sudden shift to remote work and corresponding increase in the use of remote-access software created additional data and information system vulnerabilities. The OIG's ongoing FISMA FY 2021 audits include an assessment of vulnerabilities created or exacerbated by DOJ's use of remote-access software to facilitate telework during the pandemic, and whether any such vulnerabilities were effectively mitigated.

Examples of OIG Work:

Audit of the Federal Bureau of Investigation's Strategy and Efforts to Disrupt Illegal Dark Web Activities

In December 2020, the OIG released a report examining the Federal Bureau of Investigation's (FBI) strategy and efforts to disrupt illegal dark web activitiesAmong the issues identified in the report was the challenge of how the Department can most effectively utilize finite resources to investigate cryptocurrency on the dark web. According to the FBI, investigations involving the illicit use of cryptocurrency have increased from 15 cases in 2015 to over 350 cases in 2019 and resulted in the seizure of over $100 million in cryptocurrency. We found that rising costs of cryptocurrency support for dark web investigations, particularly licensing costs for analytic tools, and static funding from the Assets Forfeiture Fund resulted in disagreement between two FBI teams on the prioritization of resources and revealed concerns that they are conducting redundant work. The OIG recommended that the FBI complete its development of the FBI-wide cryptocurrency support strategy to better address this emerging technology challenge. This strategy is still in progress as of September 2021.

Ongoing Work:

Audit of the Department's Cyber Supply Chain Risk Management Efforts

The OIG initiated an audit of DOJ's cyber supply chain risk management efforts.
The preliminary objective is to determine the extent to which the Department, through the Justice Management Division and the Federal Bureau of Investigation, implemented an organizational SCRM program that identifies, assesses, mitigates, and responds to supply chain risk throughout the information technology lifecycle.

The Department of Justice's Efforts to Coordinate the Sharing of Information Related to Malign Foreign Influence Directed at U.S. Elections

This review will assess the effectiveness and resilience of the Department's information-sharing system; evaluate the Department's oversight, management, and coordination of its activities to respond to malign foreign influence on elections; and identify any gaps in or duplication of its information sharing efforts.

Audit of the Bureau of Alcohol, Tobacco, Firearms and Explosives' monitoring of 3-D firearm printing technology

In light of the emerging technology challenge for the Department, the OIG is auditing the Bureau of Alcohol, Tobacco, Firearms and Explosives' (ATF) monitoring of 3-D firearm printing

technology. The purpose of the audit is to evaluate the effectiveness of ATF policies and procedures regarding the monitoring and mitigation of risks presented by 3-D firearms printing technology and trafficking.

Audit of the United States Marshals Service's Management of Seized Cryptocurrency
In light of the growing predominance of cryptocurrency in illegal Internet activities and the corresponding increase in cryptocurrency seizures, this emerging technology also presents the challenge of adapting traditional methods for managing seized assets. In recognition of this challenge, the OIG has initiated an audit to evaluate the U.S. Marshals Service (USMS) management of seized cryptocurrency. The audit will assess the effectiveness of USMS's policy and procedures for safeguarding, tracking, storing, valuing, and disposing of seized virtual currencies in its custody; and evaluate the USMS's plans to use a contractor to manage seized cryptocurrency.

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

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

Enhancing Trust in Police-Community Relationships
Enhancing trust is critical because a constructive relationship between the police and the communities they serve is essential to effective policing. This is not a new challenge. In FY 2020 Top Management and Performance Challenges (TMPC) report[3], the Office of the Inspector General (OIG) identified strengthening public confidence in law enforcement and protecting civil liberties as a challenge and, in the TMPC reports from 2015-2018, the OIG also identified building trust and improving police-community relations as a challenge.

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

Information sharing and coordination among federal, state, and local entities is essential in combating crime, particularly for complex domestic and international criminal activity, and remains a significant challenge for the Department. Unfortunately, several OIG reviews have identified significant issues that can arise when coordination and information sharing does not effectively occur.

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

[3] https://oig.justice.gov/reports/top-management-and-performance-challenges-facing-department-justice-2020

The Department's ability to meet and defeat the growing threat posed by transnational crime will require strategic management and robust oversight of DOJ's increasingly frequent interactions with foreign law enforcement partners. One of the Department's initiatives to combat global crime is focused on promoting the rule of law through grants and law enforcement training programs. DOJ must be careful to ensure that its expanding authorities in international arenas result in fully coordinated training and assistance with sufficient monitoring efforts. The second strategy to meet this challenge focuses on developing effective foreign law enforcement partners on whom the Department can rely on to help target and disrupt transnational drug trafficking organizations impacting the United States.

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

Continued Efforts to Reduce Gun Violence and Other Violent Crime
As the chief federal law enforcement agency, the Department has an important role in coordinating violent crime reduction efforts across the country. This role is particularly important because of the increase in violent crime in 2020 and early 2021. According to data[4] released by the FBI in September 2021, the number of murder and nonnegligent manslaughter offenses in 2020 increased 29.4 percent, and the overall violent crime rate rose 5.2 percent when compared with the 2019 rate, which is the first increase in 4 years.

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

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

Examples of OIG Work:
Investigation and Review of the Federal Bureau of Investigation's Handling of Allegations of Sexual Abuse by Former USA Gymnastics Physician Lawrence Gerard Nassar
In July 2021, the OIG's investigation and review of the FBI's handling of allegations of sexual abuse by former USA Gymnastics physician Lawrence Gerard Nassar found that FBI officials in multiple offices failed to expeditiously notify state and local law enforcement about the allegations, and other FBI field offices with stronger jurisdictional links to the allegations failed

[4] https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-2020-crime-statistics

to mitigate the ongoing danger posed by Nassar. The OIG made four recommendations to improve the FBI's processes to address the concerns identified.

Review of the Department of Justice's Planning and Implementation of Its Zero Tolerance Policy and Its Coordination with the Departments of Homeland Security and Health and Human Services

In January 2021, the OIG's report of the Department's implementation of its Zero Tolerance Policy found that DOJ leadership did not effectively coordinate with the Southwest border U.S. Attorney's Offices, USMS, U.S. Department of Health and Human Services, or the federal courts prior to urging DHS to implement the practice of referring family unit adults to DOJ for prosecution. This lack of coordination resulted in, among other things, the Department failing to carefully and appropriately consider the effects of family unit prosecutions and child separations. The OIG recommended, among other things, that prior to issuing a significant policy affecting multiple Department components, other Executive Branch agencies, or the courts, that the Department coordinate directly with affected stakeholders to ensure effective implementation.

Audit of the Drug Enforcement Administration's Headquarters-Based Oversight of its Supported Foreign Law Enforcement Units

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

Audit of the Criminal Division's Process for Incoming Mutual Legal Assistance Requests Audit Division

In July 2021, the OIG released a report that examined OIA's management of MLA requests from foreign law enforcement authorities. The OIG found that OIA is making progress in improving its process for handling incoming MLA requests but continues to be challenged by at least three main areas: (1) the high pending caseload, (2) hiring and retaining employees, and (3) an antiquated case management system. Meeting this challenge is particularly important because the failure to effectively do so could undermine the United States' ability to obtain assistance from foreign countries in critical matters involving, among others, national security, human trafficking, and information security.

7. Managing Opioids/Fentanyl Crisis

Given the Department of Justice's (DOJ or the Department) law enforcement responsibilities and the Drug Enforcement Administration's (DEA) role as a regulator of controlled substances, the widespread misuse of and addiction to opioids—including fentanyl, a powerful synthetic opioid

that is similar to morphine but 50 to 100 times more potent—is a significant challenge for the DEA and the Department given the ongoing national crisis affecting public health and the social and economic welfare of the country. The continuing challenge of confronting the opioids crisis has been heightened by the impact of the COVID-19 pandemic on drug abuse and overdose deaths.

Community-Based Strategies
In February 2021, the DEA initiated Operation Engage, which uses community-based strategies to address he illicit narcotics that present the greatest threat to public health in different communities, rather than focusing solely on opioids. Through this program, each DEA Division focuses on a designated city or region, identifies its local drug-related enforcement priorities, supports local drug use prevention efforts, and serves as a bridge between public safety and public health efforts to decrease illegal drugs.

Grants to Support Opioids Programs and Law Enforcement Efforts
The Department also plays an important role in supporting the state and local response to the opioids and fentanyl crisis through its grant awards. For example, in October 2020, DOJ announced it had awarded over $341 million in grants, adding to an already unprecedented level of Department investment targeted at fighting this national crisis. A significant portion of this grant funding (more than $147 million) was awarded to support the Bureau of Justice Assistance's Comprehensive Opioid, Stimulant and Substance Abuse Site-based Program (COSSAP) which is designed to provide financial and technical assistance to state, local, and tribal governments to develop, implement, or expand comprehensive intervention efforts for individuals impacted by opioids and other illegal drugs. One of the Department's biggest challenges in this area is ensuring that the funding it provides is accomplishing the goals of its grant programs.

Examples of OIG Work:
Review of the Drug Enforcement Administration's Regulatory and Enforcement Efforts to Control the Diversion of Opioids
In the October 2019 report, the OIG found that DEA policies and regulations did not adequately hold registrants accountable or prevent the diversion of pharmaceutical opioids. The OIG made nine recommendations to improve the Department's and the DEA's ability to combat the diversion of pharmaceutical opioids and effectively regulate registrants that engage in diversion. One of the recommendations was that the DEA develop a national prescription opioids enforcement strategy that encompasses the work of all DEA field divisions tasked with combating the diversion of controlled substances and establish performance metrics to measure the strategy's progress. As of September 2021, this recommendation and three others remain open. Progress on these open recommendations will aid in the DEA's and Department's efforts to address the challenge presented by the opioids crisis.

Audit of the Drug Enforcement Administration's Community-Based Efforts to Combat the Opioid Crisis
In September 2020, the OIG conducted an audit of the DEA's community-based efforts to combat the opioids crisis; and concluded that the program helped increase awareness of opioids-related issues, provide training, build anti-drug coalitions, and create and distribute educational materials made available for no charge. The OIG also identified areas for improvement in the DEA's pilot city selection process, allocation of resources, and collaborative efforts with other federal entities tasked with combatting the opioids crisis. We also found that the DEA lacked an

outcome-oriented performance measurement strategy to assess the effectiveness of its community outreach efforts. The OIG's recommendations will help the Department improve its collaboration with federal partners and implement a performance-based approach to maximize the impact of its community-based intervention programs.

Ongoing Work:

Audit of the Bureau of Justice Assistance Comprehensive Opioid, Stimulant, and Substance Abuse Program (COSSAP)

The OIG is conducting an audit of the Bureau of Justice Assistance (BJA) Comprehensive Opioid, Stimulant, and Substance Abuse Program (COSSAP). The preliminary objectives are to determine whether BJA: (1) implemented adequate oversight and management of COSSAP, (2) effectively coordinated and collaborated with COSSAP partners and stakeholders, and (3) accomplished COSSAP objectives and deliverables.

Audit of the Office of Community Oriented Policing Services Anti-Heroin Task Force Program (AHTF)

The OIG is assessing the COPS Office administration and oversight of the program, determining the extent to which the program has been successful, and reviewing coordination efforts between the COPS Office and other DOJ entities to combat the heroin and opioids crisis.

8. Managing Human Capital

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

Human Capital and Safety Issues Arising from the Pandemic

The COVID-19 pandemic resulted in a seismic shift in how federal employees, including Department personnel, carried out their duties. As fluctuations in the status of the COVID-19 pandemic arise, such as increasing infection rates in some locations across the county and complications from emerging variants of the virus, the Department will need to navigate a complex and changing landscape that impacts a host of human capital issues.

Recruitment, Retention, and Diversity

The wide availability of workplace flexibilities not only improve the Department's functionality during the pandemic and other emergencies, but they also increase the Department's ability to recruit and retain a highly qualified and diverse workforce.

Maintaining a Safe Workplace Environment Free from Sexual Harassment and Misconduct

The Department instituted a zero-tolerance policy regarding sexual harassment in 1993, amended the policy in 1998, and reaffirmed it in 2015, after an OIG report[5] revealed systemic issues within the Department's law enforcement components' processes for handling allegations of sexual harassment and misconduct. In addition to conveying the priority of that objective, the Department must respond promptly and appropriately to substantiated allegations of such misconduct. This work enhances the professionalism of the Department, supports victims, and deters the toxic misconduct that is antithetical to the Department's overall mission. The persistence of this issue arising throughout DOJ components, as evidenced by numerous recent OIG investigations, makes clear that this is a challenge that requires the continued vigilance of DOJ and component leadership.

Human Resource Policies

An ongoing challenge for the Department is to recruit and retain a highly qualified and diverse set of employees and to remain competitive with other federal agencies. Accomplishing this goal requires current, complete, and consistent human resource (HR) policies fundamental to the Department's HR infrastructure and human capital management.

Examples of OIG Work:

Limited-Scope Review of the Executive Office for Immigration Review's Response to the Coronavirus Disease 2019 Pandemic

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

Management Advisory Memorandum: Notification of Concerns Identified in the Department of Justice's Human Resources Policies

In August 2021, the OIG issued a Management Advisory Memorandum to the Justice Management Division detailing the Department faces the challenge of ensuring that its HR policy includes pertinent HR guidance and contains information that is consistent with current relevant regulations and OPM guidance. Among other things, the OIG found that the Department lacks a centralized location for its HR guidance, and that the Department has not fulfilled its own internal requirement to review and update its HR policies every 5 years, which has resulted in significantly outdated, and at times inaccurate, Department-wide policies. The policy issues that the OIG identified not only contribute to DOJ components' lack of knowledge of essential HR authorities and procedures, but they could weaken the Department's ability to recruit and retain highly qualified employees and to remain competitive with other federal agencies, which, as

[5] https://oig.justice.gov/reports/handling-sexual-harassment-and-misconduct-allegations-departments-law-enforcement

noted in the FY 2020 TMPC report, is a continuing challenge for the Department. In order to meet this challenge DOJ will need to address the existing deficiencies in its HR policies, monitor and update HR policies and guidelines as appropriate, evaluate its process for reviewing and updating policies, and prioritize efforts to consolidate all HR policies in a centralized location for components to reference and incorporate into their own policies.

Ongoing Work:

Review of Gender Equity in the FBI's Training and Selection Processes for New Special Agents and Intelligence Analysts at the FBI Academy

The OIG is conducting a review to assess gender equity in the training and selection process for new Special Agents and Intelligence Analysts. The review will examine policies and practices, trends and patterns for male and female trainees, and perceptions of gender equity at the FBI Academy. It will also assess processes designed to ensure gender equity and prevent gender discrimination for trainees, including the FBI's internal Equal Employment Opportunity process.

Review of Racial Equity in the Department of Justice's Law Enforcement Components

To further assist the law enforcement components and promote a diverse workforce, in this review the OIG will assess equity across race, color, national origin, and ethnicity by reviewing component demographics, recruitment, hiring, retention, attrition, promotions, and awards. This review will also include a survey assessing staff perceptions related to equity.

Findings of Misconduct by an FBI Assistant Special Agent in Charge for Engaging in Unwanted Sexual Contact With and Making Offensive Sexual Comments to FBI Employees and Consuming and Providing Alcohol to Subordinates and Visitors While on Duty

In January 2021, the OIG reported that a Federal Bureau of Investigation (FBI) Assistant Special Agent in Charge engaged in unwanted sexual touching with three FBI employees, created a hostile work environment by engaging in that unwanted physical sexual contact and making offensive sexual comments to FBI employees. The OIG found that this conduct violated the Department's zero tolerance policy regarding sexual harassment, as well as FBI policies regarding sexual harassment and employee conduct.

Investigative Summary: Findings of Misconduct by an Assistant United States Attorney for Sexually Inappropriate Comments to Multiple Individuals, Inappropriate Touching of an Intern's Breast, and Lack of Candor to the OIG

In November 2020, the OIG found that an Assistant U.S. Attorney engaged in sexually harassing conduct by making sexually inappropriate comments to an intern, an Assistant U.S. Attorney, and two other individuals, and also by inappropriately touching the intern's breast. The OIG found that this conduct violated the zero-tolerance policy and state law.

9. Ensuring Financial Accountability of Department Contracts and Grants

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

Effective contract oversight ensures that the Department receives products and services that fulfill its mission while detecting fraud, waste, and abuse when spending taxpayer dollars. In numerous individual contract audits over the past several years, the OIG has repeatedly identified weaknesses in DOJ's management and administration of its contracts, including inadequate acquisition planning, acceptance and payment of unallowable costs, inadequate monitoring of contract performance, and inadequate training of government personnel assisting with contract administration and oversight.

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

Examples of OIG Work:

Procurement Issues at the Federal Bureau of Prisons

Procurement issues continue to challenge BOP. In the FY 2020 TMPC report, we noted the OIG's concerns over how the BOP procures food, including issues related to pre-award diligence, contractor performance, and quality controls. The purchase of food products that do not meet applicable standards potentially endangers the health and safety of BOP inmates and staff. Further, addressing this issue is important for BOP financial accountability in procurements, which account for a substantial portion of the BOP's budget. For example, in FY 2019, the BOP allocated 5.7 percent or approximately $401 million of its budget to food products and food services for the roughly 180,000 inmates housed in 122 BOP institutions. These challenges with food procurement were summarized in a Management Advisory Memorandum reissued by the OIG in 2020 and were evident in a False Claims Act settlement in January 2021 that resolved allegations regarding the sale of adulterated or substandard food products to the BOP.

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

potentially fraudulent claims and, because most of the BOP's healthcare claims are processed by paper at individual institutions, billing across the BOP cannot be meaningfully analyzed.

Management Advisory Memorandum Concerning the Department of Justice's Administration and Oversight of Contract

The Department's recurring contract oversight issues led the OIG to issue a Management Advisory Memorandum in July 2020. This memorandum summarized the deficiencies the OIG identified and recommendations that the Department consider including contract management in its enterprise-level risk management prioritization. As the OIG's oversight findings reflect, contract oversight remains an important challenge facing the Department.

Audit of the Drug Enforcement Administration's Laboratory Information Management System Support Contracts

In June 2021, OIG issued an audit report on the DEA Laboratory Information Management System support contracts underscored many of the deficiencies that were highlighted in the OIG's July 2020 Management Advisory Memorandum. Among other things, the report found that the DEA did not adhere to the FAR and the DEA's internal policy, which require contracting officials to develop and implement a quality assurance surveillance plan along with the statement of work to monitor the contractor's performance, and that the DEA failed to consistently conduct or document the results of contractor performance evaluations. The contract also did not include required whistleblower protections clauses, which was a systemic issue the OIG notified the Department about in a February 2021 Management Advisory Memorandum concerning the Department's compliance with laws, regulations, and policies regarding whistleblower rights and protections for contract workers supporting Department programs.

Findings of Misconduct by a then FBI Special Agent in Charge and two then FBI Assistant Special Agents in Charge for Their Roles in an Unauthorized $2 Million Purchase of Intellectual Property Related to a Classified Undercover Operation and Related Misconduct

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

Audit of Certain Tax Division Contracts Awarded for Expert Witness Services

In September 2021, the OIG issued an audit report regarding Tax Division contracts awarded for expert witness services that identified areas of non-compliance with the FAR and internal guidance. One of the findings was that trial attorneys who were expected to handle significant contracting activities were not formally designated these responsibilities, were not trained as required by the FAR, and did not display the requisite knowledge of FAR requirements to undertake certain contract procurement and oversight tasks.

Audit of the Environment and Natural Resources Division's Procurement and Administration of Expert Witness Contracts

In September 2020, OIG issued an audit report regarding the Environment and Natural Resource's Division's procurement and administration of expert witness contracts. Our report contains eight recommendations for ENRD and one recommendation for JMD

Report on the USMS' Contract with The GEO Group, Inc. for the Robert A. Deyton Detention Facility in Lovejoy, Georgia

In an audit report issued July 2020 regarding the U.S. Marshals Service's (USMS) contract to operate a detention facility, the OIG found that the USMS needs to improve its contract oversight procedures, particularly regarding unmet staffing levels, processing invoice deductions, contract price reduction proposals, and the use of commissary funds. As of September 2021, 5 of the 10 recommendations remain open.

Management Advisory Memorandum: Notification of Concerns Identified in Connection with the Federal Bureau of Prisons' Procurement of Air Ambulance Services

In April 2021, the OIG expresses concern about how the BOP procures air ambulance services. The absence of uniform guidance or contract provisions concerning reimbursement for air ambulance claims has resulted in inconsistent handling of air ambulance claims across BOP institutions and the BOP in many cases has reimbursed air ambulance claims at rates far in excess of the Medicare reimbursement rates.

Audit of the Federal Bureau of Prisons' Perimeter Security Strategy and Efforts Related to the Contract Awarded to DeTekion Security Systems, Incorporated, to Update the Lethal/Non-Lethal Fence at Nine United States Penitentiaries

In September 2020, an OIG audit report identified several deficiencies in the contracting process related to a $3.2 million contract to update fences at nine U.S. Penitentiaries. The OIG found that the BOP did not perform an adequate price proposal analysis to determine whether the contract had a fair and reasonable price. As a result, the OIG estimated that the contractor received from BOP over $900,000 in additional profit because the project took significantly less time to complete than estimated for the firm-fixed-price contract.

Audit of the Office of Justice Programs Victim Assistance Grants Awarded to the Kentucky Justice and Public Safety Cabinet, Frankfort, Kentucky

In September 2021, the audit found, among other things, that the grantee did not complete its monitoring activities on a timely basis and performed inadequate oversight of subrecipient financial reporting and matching funds. The report also identified over $1.5 million in questioned costs. These issues demonstrate how poor financial monitoring can increase the risk that government funds will not be used in compliance with federal regulations. In meeting this challenge, the Department must remain vigilant in its instructions to and oversight of grantees to ensure taxpayer funds are expended for the intended purpose, and to advance the objectives of the grant program.

Review of the Office of Justice Programs' Administration of CARES Act Funding

In September 2021, the OIG issued the final audit report. The review found, among other things, that OJP acted quickly to distribute CESF funding and that most recipient spending reviewed appeared allowable under the terms and conditions of the awards. However, the report noted that, as of March 31, 2021, CESF recipients reported spending or obligating only 40 percent of the total amount awarded and OJP must continue to carefully monitor CESF funds to ensure they are spent in the manner intended.

Ongoing Work:

Audit of Office of Justice Programs' Contract Awarded for the JustGrants System

The OIG is conducting an audit of OJP's contract for the Justice Grants System (JustGrants). The contract was initially awarded to CSRA LLC, which was subsequently acquired by General Dynamics. The preliminary objectives of the audit are to assess: (1) OJP's implementation of the JustGrants transition; (2) OJP's administration of the contract; and (3) CSRA LLC's performance and compliance with the terms, conditions, laws, and regulations applicable to the contract.

Audit of the Criminal Division's and the Executive Office of the U.S. Attorneys' Management and Coordination of Pandemic-related Fraud Allegations and Referrals

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

10. Whistleblower Program

Whistleblowers perform an important service for the public and DOJ when they report evidence of wrongdoing. All DOJ employees, contractors, subcontractors, grantees, subgrantees, and personal services contractors are protected from retaliation for making a protected disclosure. Reports concerning wrongdoing by DOJ employees or within DOJ programs can always be submitted directly to the OIG Hotline.

The Whistleblower Program continues to play a leadership role in the Council of Inspectors General on Integrity and Efficiency's (CIGIE) efforts to educate and empower whistleblowers to come forward with lawful disclosures of misconduct. The OIG's Whistleblower Protection Program led a CIGIE effort to develop an online tool for whistleblowers, at www.oversight.gov/whistleblowers, that allows users to respond to a few simple prompts, and they are then directed to the appropriate Inspector General, the Office of Special Counsel (OSC), or other entity to report wrongdoing or to file a retaliation complaint. The site also provides specific information to individuals in various sectors, such as whistleblower protections for contractors and grantees, members of the military services, and intelligence community employees. The DOJ OIG also continues to Chair an CIGIE working group on whistleblower protections that meets quarterly to discuss and develop best practices in the administration of whistleblower programs throughout the IG community.

Whistleblower Protection Coordinator:

The IG Act requires the DOJ OIG to designate an individual to serve as the OIG's Whistleblower Protection Coordinator. The OIG's Whistleblower Protection Coordinator carries out several key functions, including:

- Educating DOJ employees and managers about prohibitions on retaliation for protected disclosures;
- Educating employees who have made or are contemplating making a protected disclosure about the rights and remedies available to them;

- Ensuring that the OIG is promptly and thoroughly reviewing complaints that it receives, and that it is communicating effectively with whistleblowers throughout the process; and
- Coordinating with the OSC, other agencies, and non-governmental organizations on relevant matters.

For more information, contact the OIG Whistleblower Protection Coordinator Program.

The DOJ OIG also continues to utilize the tracking system developed through the OIG Ombudsperson Program to ensure that it is handling these important matters in a timely manner. The DOJ OIG continuously enhances the content on its public website, oig.justice.gov. The table below, pulled from our *Semiannual Report to Congress, April 1, 2021 through September 30, 2021,* presents important information.

Whistleblower Program
April 1, 2021 – September 30, 2021

Employee complaints received	199
Employee complaints opened for investigation by the OIG	54
Employee complaints that were referred by the OIG to the components for investigation	89
Employee complaint cases closed by the OIG	69

Whistleblowers perform a critical role when they bring forward evidence of wrongdoing and they should never suffer reprisal for doing so. The OIG Whistleblower Protection Coordinator Program (the Whistleblower Program) works to ensure that whistleblowers are fully informed of their rights and protections from reprisal.

In July 2021, DOJ Inspector General Michael Horowitz participated as an honorary speaker at the annual National Whistleblower Day event, and was joined by Senator Charles Grassley, Senator Ron Wyden, Representative Jackie Speier, Secretary of Labor Marty Walsh, and many others in support of the event's primary goal: celebrating the accomplishments of whistleblowers and their efforts to fight corruption, waste, and other crimes.

At this year's event, Inspector General Horowitz discussed his role as Chair of the PRAC, to highlight the PRAC's work fighting waste, fraud, and abuse in pandemic spending. With trillions of dollars going to millions of recipients, Inspector General Horowitz noted that whistleblowers are a critical part of the effort to ensure that these funds go to their intended recipients, promote economic recovery, and improve public health providers, and are not wasted or misspent by individuals or corporations or others looking to take advantage of the unprecedented increase in federal spending. For more information on the PRAC's work, visit their website.

11. Congressional Testimony

The Inspector General testified before Congress on the following occasions:

- Statement of Michael E. Horowitz, Inspector General, U.S. Department of Justice before the U.S. Senate Committee on Homeland Security and Governmental Affairs concerning "Safeguarding Inspector General Independence and Integrity on October 21, 2021.
- Dereliction of Duty: Examining the Inspector General's Report on the FBI's Handling of the Larry Nassar Investigation" before the U.S. Senate Committee on the Judiciary on September 15, 2021.
- "Assessing the Federal Government's COVID-19 Relief and Response Efforts and its Impact" before the U.S. House of Representatives Committee on the Transportation and Infrastructure on July 29, 2021.
- "The Pandemic Response Accountability Committee's Role in Combating Fraud in Pandemic Relief and Small Business Programs" before the U.S. House of Representatives Committee on Oversight and Reform, Select Subcommittee on the Coronavirus Crisis on March 15, 2021.
- "Management, Performance Challenges, and COVID Response at the Department of Justice" before the U.S. House of Representatives, Subcommittee on Commerce, Justice, Science and Related Agencies on March 24, 2021;
- "Accountability and Lessons Learned from the Trump Administration's Child Separation Policy" before the U.S. House of Representatives Committee on Oversight and Reform on February 4, 2021;

E. Challenges

Like other organizations, the OIG must confront a variety of internal and external challenges that affect its work and impede progress towards achievement of its goals. These include decisions made by Department employees while carrying out their numerous and diverse duties, which affect the number of allegations the OIG receives, and financial support from the OMB and Congress.

The limitation on the OIG's jurisdiction has also been an ongoing impediment to strong and effective independent oversight over agency operations. While the OIG has jurisdiction to review alleged misconduct by non-lawyers in the Department, it does not have jurisdiction over alleged misconduct committed by Department attorneys when they act in their capacity as lawyers—namely, when they are litigating, investigating, or providing legal advice. In those instances, the IG Act grants exclusive investigative authority to the Department's OPR office. As a result, these types of misconduct allegations against Department lawyers, including any that may be made against the most senior Department lawyers (including those in departmental leadership positions), are handled differently than those made against agents or other Department employees. The OIG has long questioned this distinction between the treatment of misconduct by attorneys acting in their legal capacity and misconduct by others. This disciplinary system cannot help but have a detrimental effect on the public's confidence in the Department's ability to review misconduct by its own attorneys.

The OIG's greatest asset is its highly dedicated personnel, so strategic management of human capital is paramount to achieving organizational performance goals. In this competitive job market, the OIG must make every effort to maintain and retain its talented workforce. The OIG's focus on ensuring that its employees have the appropriate training and analytical and technological skills for the OIG's mission will continue to bolster its reputation as a premier federal workplace and improve retention and results.

II. Summary of Program Changes

Item Name	Description	Pos.	FTE	Dollars ($000)	Page
Information Technology (IT) Enhancements	The OIG requests a program enhancement of $3.626 million to continue to modernize and enhance the security of its technology operations.	0	0	$3,626.0	32
Office of Data Analytics Enhancement	The OIG requests a program increase of funding to support the Office of Data Analytics. The role of data analytics has expanded in recent years and has proven essential in evaluating risk and identifying fraud, waste and abuse in contracts, grants, healthcare costs, and other Department programs.	0	0	$1,200.0	38
Cyber Forensics, Data Analytics, Special Reviews and Operation Enhancement	The OIG requests a program enhancement of $3.950 million to support its effort in overseeing emerging and high-risk areas in which the Department must operate optimally to ensure the security of the nation and sound stewardship of American taxpayer dollars.	21	21	$3,950.0	43
Total		**21**	**21**	**$8,776.0**	

III. Appropriations Language and Analysis of Appropriations Language

The appropriation language states the following for the OIG:

For necessary expenses of the Office of Inspector General, $135,856,000 including not to exceed $10,000 to meet unforeseen emergencies of a confidential character: Provided, that not to exceed $4,000,000 shall remain available until September 30, 2024.

(Department of Justice Appropriations Act, 2023)

Provided, That notwithstanding section 1402(d) of such Act, of the amounts available from the Fund for obligation: (1) $10,000,000 shall be transferred to the Department of Justice Office of Inspector General and remain available until expended for oversight and auditing purposes associated with this section; and (2) 5 percent shall be available to the Office for Victims of Crime for grants, consistent with the requirements of the Victims of Crime Act, to Indian tribes to improve services for victims of crime.

A. Analysis of Appropriations Language

OIG is requesting that the "not to exceed" amount be increased to $6 million to support, additional investments in information technology and facilities.

IV. Program Activity Justification

A. Audits, Inspections, Investigations, and Reviews

Program Increases

OIG	Direct Pos.	Direct FTE	Amount
2021 Enacted	491	466	$120,565
2022 President's Budget	539	529	$137,184
Adjustments to Base and Technical Adjustments	0	0	($104)
2023 Current Services	539	529	$137,080
2023 Program Increases	21	21	$8,776
2023 Request	560	550	$145,856
Total Change 2022-2023	21	21	$8,672

B. Program Description

The OIG operates as a single decision unit encompassing audits, inspections, investigations, and reviews.

C. Performance and Resource Tables

PERFORMANCE AND RESOURCES TABLE (Goal 1)												
Decision Unit: OIG/Audits, Inspections, Investigations, and Reviews												
DOJ Strategic Plan Goal #1: Uphold The Rule Of Law. Objective 1.2 Promote Good Government												
OIG General Goal #1: Detect and deter misconduct in programs and operations within or financed by the Department												
WORKLOAD/RESOURCES	**FY2020**		**FY2021**				**FY2022**				**FY2023**	
	Actuals		**Projected**		**Actuals**		**Projected**		**Actuals through Quarter 1**		**Projected**	
Total Costs and FTE	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
(reimbursable FTE are included, but annual reimbursable costs are bracketed and not included in the total)	505	$105,000	466	$120,565	466	$120,565	539	$137,184	539	$137,184	560	$145,310
	68	[$14,669]	68	[$15,051]	68	[$15,372]	21	[$15,375]	21	[$15,375]	21	[$15,683]
Performance Measure												
Number of Cases Opened per 1,000 DOJ employees:												
Fraud*		0.56		*		0.42		*		0.06		*
Bribery*		0.10		*		0.11		*		*		*
Rights Violations*		0.10		*		0.09		*		0.04		*
Sexual Crimes*		0.21		*		0.07		*		0.04		*
Official Misconduct*		0.86		*		0.79		*		0.15		*
Theft*		0.06		*		0.05		*		0.03		*
Workload												
Integrity Briefings/Presentations to DOJ employees and other stakeholders		143		70		69		70		1		70
DOJ employees and stakeholders at Integrity Briefings		8,369		3,000		2,695		3,000		5		3,000
* Indicators for which the OIG only reports actuals.												

Note: FY 2018 - FY 2022, DOJ Strategic Plan: Goal 4: Strategic Objective 4.1: Uphold the rule of law and integrity in the proper administration of justice.

PERFORMANCE AND RESOURCES TABLE (Goal 1) (continued)												
Decision Unit: OIG/Audits, Inspections, Investigations, and Reviews												
DOJ Strategic Plan Goal #1: Uphold The Rule Of Law. Objective 1.2 Promote Good Government												
OIG General Goal #1: Detect and deter misconduct in programs and operations within or financed by the Department												
WORKLOAD/RESOURCES	**FY2020**		**FY2021**				**FY2022**				**FY2023**	
	Actuals		**Projected**		**Actuals**		**Projected**		**Actuals through Quarter 1**		**Projected**	
Total Costs and FTE	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
(reimbursable FTE are included, but annual reimbursable costs are bracketed and not included in the total)	505 68	$105,000 [$14,669]	466 68	$120,565 [$15,051]	466 68	$120,565 [$15,372]	529 20	$137,184 [$15,375]	539 21	$137,184 [$15,375]	560 21	$145,310 [$15,683]
Performance Measure												
Intermediate Outcome												
Percentage of BOP Investigations closed or referred for prosecution within 6 months of being opened **[Refined Measure]**		92%		75%		86% (95/110)		75%		100% (23/23)		75%
Number of closed Investigations substantiated*		157		*		$158		*		$40		*
Arrests *		89		*		$84		*		$26		*
End Outcome												
Convictions *		50		*		$97		*		$7		*
Administrative Actions *		138		*		$142		*		$20		*
Response to Customer Surveys:												
Report completed in a timely manner (%)		98%		90%		100% (77/77)		90%		100% (10/10)		90%
Issues were sufficiently addressed (%)		100%		90%		99% (76/77)		90%		100% (10/10)		90%
* Indicators for which the OIG only reports actuals.												

Note: FY 2018 - FY 2022, DOJ Strategic Plan: Goal 4: Strategic Objective 4.1: Uphold the rule of law and integrity in the proper administration of justice.

PERFORMANCE AND RESOURCES TABLE (Goal 1) (continued)
Decision Unit/Program: OIG/Audits, Inspections, Investigations, and Reviews
DOJ Strategic Plan Goal #1: Uphold The Rule Of Law. Objective 1.2 Promote Good Government
OIG General Goal #1: Detect and deter misconduct in programs and operations within or financed by the Department
Data Definition, Validation, Verification, and Limitations

A. Data Definition:

The OIG does not project targets and only reports actuals for workload measures, the number of closed investigations substantiated, arrests, convictions, and administrative actions. The number of convictions and administrative actions are not subsets of the number of closed investigations substantiated.

B. Data Sources, Validation, Verification, and Limitations:

Investigations Data Management System (IDMS) – consists of a web-based relational database systems. It's a case and document management system.

The database administrator runs routine maintenance programs against the database. Database maintenance plans are in place to examine the internal physical structure of the database, backup the database and transaction logs, handle index tuning, manage database alerts, and repair the database if necessary. Currently, the general database backup is scheduled nightly and the transaction log is backed up in 3 hour intervals. We have upgraded to a web based technology.

Investigations Division Report of Investigation (ROI) Tracking System - a web-based SQL-Server application that tracks all aspects of the ROI lifecycle. The ROI and Abbreviated Report of Investigation (AROI) are the culmination of OIG investigations and are submitted to DOJ components. These reports are typically drafted by an agent and go through reviews at the Field Office and at Headquarters levels before final approval by Headquarters. The ROI Tracking System reads data from IDMS. By providing up-to-the-minute ROI status information, the Tracking System is a key tool in improving the timeliness of the Division's reports. The ROI Tracking System also documents the administration of customer satisfaction questionnaires sent with each completed investigative report to components and includes all historical sent with each completed investigative report to components and includes all historical data. The system captures descriptive information as well as questionnaire responses. Descriptive information includes the questionnaire form administered, distribution and receipt dates, and component and responding official. The database records responses to several open-ended questions seeking more information on deficiencies noted by respondents and whether a case was referred for administrative action and its outcome. Questionnaire responses are returned to Investigations Headquarters and are manually entered into the Tracking System by Headquarters personnel. No data validation tools, such as double key entry, are used though responses are entered through a custom form in an effort to ease input and reduce errors.

Investigations Division Investigative Activity Report – Most of the data for this report is collected in IDMS. The use of certain investigative techniques and integrity briefing activities are also tracked externally by appropriate Headquarters staff.

In late FY 2021, the OIG has selected a new case management system to replace IDMS and the ROI Tracking System to streamline the administrative process for investigations.

C. FY 2020 Performance Report:

The workload measure "Investigations Closed" is no longer being tracked as of FY20. The OIG is focusing on more complex and document-intensive cases (e.g., grant and contract fraud) that require more in-depth financial and forensic analysis.

Note: FY 2018 - FY 2022, DOJ Strategic Plan: Goal 4: Strategic Objective 4.1: Uphold the rule of law and integrity in the proper administration of justice.

PERFORMANCE AND RESOURCES TABLE (Goal 2)										
Decision Unit: OIG/Audits, Inspections, Investigations, and Reviews										
DOJ Strategic Plan Goal #1: Uphold The Rule Of Law. Objective 1.2 Promote Good Government										
OIG General Goal #2: Promote the efficiency and effectiveness of Department programs and operations.										
WORKLOAD/RESOURCES	**FY2020**		**FY2021**		**FY2022**				**FY2023**	
	Actuals		**Actuals**		**Projected**		**Actuals through Quarter 1**		**Projected**	
Total Costs and FTE	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
(annual reimbursable costs are bracketed and not included in the total)	505 68	$105,000 [$14,669]	466 68	$120,565 [$15,372]	539 21	$137,184 [$15,375]	539 21	$137,184 [$15,375]	560 21	$145,310 [$15,683]
Performance Measure										
Workload										
Audit and E&I assignments initiated	Audit Only E&I Only	108 23	Audit Only E&I Only	115 9		99	Audit Only E&I Only	16 2		99
Percent of CSITAO* resources devoted to security reviews of major DOJ information systems		91%		98%		80%		93%		80%
Percent of internal DOJ audit reports that assess component performance measures		72%		82%		60%		78%		60%
Percentage of E&I assignments opened and initiated during the fiscal year devoted to Top Management Challenges		100%		100%		70%		100%		70%
Percent of direct resources devoted to audit products related to Top Management Challenges, and GAO and JMD-identified High-Risk Areas		94%		93%		85%		96%		85%
Intermediate Outcome										
Audit and E&I assignments completed	Audit Only E&I Only	103 7	Audit Only E&I Only	113 18		99	Audit Only E&I Only	21 2		99
*Computer Security & Information Technology Audit Office										

Note: FY 2018 - FY 2022, DOJ Strategic Plan: Goal 4: Strategic Objective 4.1: Uphold the rule of law and integrity in the proper administration of justice.

PERFORMANCE AND RESOURCES TABLE (Goal 2) (continued)										
Decision Unit: OIG/Audits, Inspections, Investigations, and Reviews										
DOJ Strategic Plan Goal #1: Uphold The Rule Of Law. Objective 1.2 Promote Good Government										
OIG General Goal #2: Promote the efficiency and effectiveness of Department programs and operations.										
WORKLOAD/RESOURCES	**FY2020**		**FY2021**		**FY2022**				**FY2023**	
	Actuals		**Actuals**		**Projected**		**Actuals through Quarter 1**		**Projected**	
Total Costs and FTE	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
(annual reimbursable costs are bracketed and not included in the total)	505	$105,000	466	$120,565	539	$137,184	539	$137,184	560	$145,310
	68	[$14,669]	68	[$15,372]	21	[$15,375]	21	[$15,375]	21	[$15,683]
Performance Measure										
Intermediate Outcome										
Percent of Audit resources devoted to reviews of contracts and contract management		8%		11%		5%-8%		12%		5%-8%
Components receiving information system audits		11		11		6		7		6
Percent of products issued to the Dept. or other Federal entities containing significant findings or information for management decision-making by Audit and E&I	Audit Only	90/92 100%	Audit Only	94/94 100%	Audit Only	90%	Audit Only	21/21 100%	Audit Only	90%
	E&I Only	7/7 100%	E&I Only	15/15 100%	E&I Only	6/7 86%	E&I Only	2/2 100%	E&I Only	6/7 86%
Percent of more complex internal DOJ (E&I) reviews to be provided to the IG as a working draft within an average of 12 months		71%		85%		35%		100%		35%
Percent of grant, CODIS, equitable sharing, and other external audits to be completed in draft within 8 months		81%		39%		40%		60%		40%
Percent of internal DOJ audits to be provided to the IG as a working draft within 13 months		92%		95%		60%		100%		60%

Note: FY 2018 - FY 2022, DOJ Strategic Plan: Goal 4: Strategic Objective 4.1: Uphold the rule of law and integrity in the proper administration of justice.

PERFORMANCE AND RESOURCES TABLE (Goal 2) (continued)
Decision Unit: OIG/Audits, Inspections, Investigations, and Reviews
DOJ Strategic Plan Goal #1: Uphold The Rule Of Law. Objective 1.2 Promote Good Government
OIG General Goal #2: Promote the efficiency and effectiveness of Department programs and operations.
Data Definition, Validation, Verification, and Limitations

A. Data Definition:

"Assignment" covers all audits (including internals, CFO Act, and externals, but **not** Single Audits), evaluations, and inspections. "Assignments" may also include activities that do not result in a report or product (e.g., a memorandum to file rather than a report); or reviews initiated and then cancelled.

B. Data Sources, Validation, Verification, and Limitations:

Project Resolution and Tracking (PRT) system- PRT was implemented on April 18, 2011; this OIG system was designed to track audits, evaluations, and reviews from initiation to completion, including the status of recommendations. The system provides senior management with the data to respond to information requests and track and report on current status of work activities.

C. FY 2020 Performance Report: N/A

Note: FY 2018 - FY 2022, DOJ Strategic Plan: Goal 4: Strategic Objective 4.1: Uphold the rule of law and integrity in the proper administration of justice.

V. Performance, Resources, and Strategies

A. Performance Plan and Report for Outcomes

As illustrated in the preceding Performance and Resources Tables, the OIG helps the Department achieve its strategic goals and promotes efficiency, integrity, economy, and effectiveness through its audits, inspections, investigations, and reviews. For the Department's programs and activities to be effective, Department personnel, contractors, and grantees must conduct themselves in accordance with the highest standards of integrity, accountability, and efficiency. The OIG investigates alleged violations of criminal and civil laws, regulations, and ethical standards arising from the conduct of the Department's employees in their numerous and diverse activities.

The OIG continues to review its performance measures and targets, especially in light of the changing nature of the cases it investigates, and the Department programs it audits and reviews. Today's work is much more complex and expansive than it was only a few years ago. The number of documents to be reviewed, the number of people to interview, the amount of data to examine, and the analytical work involved in many OIG products are significantly greater than in prior years. The OIG ensures sufficient time and resources are devoted to produce high-quality, well-respected work.

B. Strategies to Accomplish Outcomes

The OIG will devote all resources necessary to investigate allegations of bribery, fraud, abuse, civil rights violations, and violations of other laws and procedures that govern Department employees, contractors, and grantees, and will develop cases for criminal prosecution and civil and administrative action. The OIG will continue to use its audit, inspection, evaluation, and attorney resources to review Department programs or activities identified as high-priority areas in the Department's Strategic Plan and focus its resources to review the Department's TMPC.

VI. Program Increases by Item

<table>
<tr><th colspan="5">A. Item Name: Information Technology (IT) Enhancements</th></tr>
<tr><td>DOJ Strategic Plan Goal #1: Uphold The Rule Of Law. Objective 1.2 Promote Good Government</td><td colspan="4">DOJ Strategic Plan Goal #1: Uphold The Rule Of Law. Objective 1.2 Promote Good Government</td></tr>
<tr><td>Organizational Program:</td><td colspan="4">OIG</td></tr>
<tr><td rowspan="2">Program Increase:</td><td>Positions 0</td><td>Agt/Atty 0/0</td><td>FTE 0</td><td>Dollars $0</td></tr>
<tr><td colspan="2">Equipment/software/services:</td><td colspan="2">Dollars $3,626,000</td></tr>
<tr><td>Total Request of Increase:</td><td colspan="4">$3,626,000</td></tr>
</table>

1. Description of Item

On May 12, 2021, the President issued an Executive Order on Improving the Nation's Cybersecurity stating, "The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors." To meet this Executive Order and continue to promote integrity, efficiency, accountability, and good government through robust independent oversight, the OIG requires a program enhancement of **$3.626 million** to continue to modernize its information technology infrastructure and cybersecurity posture. The program enhancement focuses on three crucial areas for improving the OIG's cybersecurity posture: (1) modernizing the OIG's IT infrastructure through the deployment of secure web gateways, software defined networks, secure wireless guest networks, physical access control systems, and creating a multi-cloud strategy; (2) enhancing the OIG's security footprint by deploying cybersecurity software tools such as Microsoft E5, Varonis, Okta, and Network Access Control (NAC); and (3) modernizing the OIG cybersecurity investigations technology with a forensic virtualization platform and replacement digital forensic case management system.

2. Justification

The OIG requests the specific program enhancements described below to support its ongoing IT cybersecurity modernization initiative and achieve its mission to promote integrity, efficiency, and accountability within the DOJ.

(1) Modernizing the IT Infrastructure - $1.771M

Secure Web Gateways - $100K

As the OIG continues to operate in the Microsoft Azure Government Cloud Environment and leverages DOJ virtual private network (VPN) technology to support a larger remote workforce, there is an immediate need to implement cybersecurity systems designed to protect OIG data and enforce security policies. This systems enhancement allows the OIG to replace current VPN technology with an upgraded secure web gateway system, resulting in a better customer connectivity experience with faster performance to meet the needs of the OIG remote workforce, while gaining added cybersecurity safeguards around OIG data when creating remote connections.

Software Defined Networks - $721K

The OIG utilizes the DOJ Justice Unified Telecommunications Network (JUTNET) to provide wide-area network (WAN) services to its Headquarters (HQ) and 16 regional field offices. The Multiprotocol Label Switching VPN (MPLS) backbone of JUTNET is costly to maintain and operate as it requires on-site maintenance and support, and it is not easily scalable to meet the increasing demands of the OIG mission. Additionally, there are performance issues with file transfers between JUTNET and the Microsoft Azure Government Cloud Environment that extend operational timelines for the OIG workforce. This program enhancement allows the OIG to design and implement a Software Defined Network to replace the current JUTNET infrastructure. A Software Defined Network offers the OIG ease of hardware deployment, central manageability, mission scalability, and improved connectivity for faster file sharing and data uploads. It also adds more cybersecurity capabilities for monitoring the WAN, which our current JUTNET infrastructure does not provide.

Secure Guest Networks - $200K

Currently, the OIG does not have secure guest networks to support collaboration between the OIG and other DOJ components or law enforcement agencies. As a result, OIG guests to OIG Investigations Division field locations, such guests primarily being other DOJ employees such as EOUSA personnel and DOJ law enforcement agents, have been required to sign into unsecure public Wi-Fi or collaborate in public settings with Wi-Fi capabilities resulting in potential exposures of OIG casework to the public. Establishing secure guest networks would allow for more secure performance of OIG mission work by allowing OIG guests to connect to the internet and collaborate with OIG personnel on current and future cases in an environment that affords the appropriate level of security for OIG and DOJ information. This program enhancement allows the OIG to establish secure guest networks at eight OIG field offices. This capability would also support cyber investigations by providing a test and evaluation capability for zero trust technology solutions in the OIG field offices.

Physical Access Control System (PACS) - $500K

Pursuant to HSPD-12, FIPS 201, and FISMA, physical access control devices are required at all OIG locations. However, the current PACS installed across OIG's 18 field, area, and regional audit offices has either a) aged beyond repair, b) reached end of life, or c) is non-existent – eight (8) sites lack FIPS-compliant systems, nullifying their viability and compliance. Further, the

existing OIG PACS suffers from using four (4) different PACS software across OIG's 18 field, area, and regional offices, resulting in compatibility issues and increased level of effort to maintain; a single, unified, enterprise-wide system would alleviate these and other concerns. That software system (currently used in only 50% of OIG offices), which the OIG would install with this funding request, is the C-CURE 9000 security software solution. Specifically, implemented across all OIG locations, C-CURE 9000 would create a secure, remote Enterprise PACS (E-PACS) server. From its Washington, D.C. headquarters (HQ), E-PACS will allow the OIG's Office of Security Programs (OSP) to monitor and control access to all OIG sites and ensure each site's FISMA and FIPS compliancy. HQ-administered monitoring will enable centralized management of all remote office PACS, reducing burden on individual offices across the country while improving system and security oversight. Insider threat scenarios, anomalous activity, penetrated space and potential forced entry will be centrally monitored as a backstop to the on-site physical security countermeasure protocols at each of the OIG's nationwide physical locations. Reporting will improve consolidated, holistic, OIG-wide facility reports that can be generated to inform future security decision making. Lacking E-PACS, with 11 of the OIG's 18 remote offices being leased, non-government facilities, and continuing to rely on non-federally compliant systems that are well-beyond their useful life, jeopardize the security and safety of the OIG's remote offices: information, personnel, and the facility itself will be vulnerable.

Multi-Cloud Environment - $250K

In FY 2019, the OIG migrated its core enterprise IT services to the Microsoft Azure Government Cloud environment and will finalize migrating the remainder of its IT services to the Azure Cloud in FY 2022 in support of the Federal Cloud Computing Strategy based on the need to consolidate data centers, provide redundancy in the cloud operating environment, safeguard OIG data, and ensure continuity of operations. As the threat of ransomware attacks grows daily, the OIG is required to harden its cybersecurity posture. This program enhancement allows the OIG to develop a multi-cloud strategy as a countermeasure to ransomware attacks and ensures OIG data is protected and duplicated with a secondary cloud provider to the Microsoft Azure Government Cloud Environment.

(2) Enhancing the Security Footprint - $355K

In the last year, the Federal Government saw an immediate need to increase security around government IT infrastructures to safeguard data and networks. To meet this need and enhance the security footprint, the OIG requires this program enhancement to deploy cybersecurity software tools such as Microsoft E5, Varonis, Okta, and Network Access Control (NAC).

The OIG currently utilizes the Microsoft E3 licensing structure; however, by migrating Microsoft licenses to E5, the OIG adds many advanced organizational capabilities for the OIG workforce, including enhanced threat protection required to safeguard OIG data. In addition to the security benefits, this migration provides the OIG with advanced eDiscovery capabilities, enhanced collaboration tools, and telecom flexibility, creating a simplified ecosystem to manage, monitor, and provide safe services.

Deploying a data security software platform, much like the Varonis software tool, provides the OIG total visibility and control over managing and safeguarding agency data. Through this software tool, the OIG can protect sensitive data, detect sophisticated threats, and streamline

privacy and compliance regulations. Additionally, the OIG can actively monitor data to create a more robust data governance policy through better understanding of data usage.

The OIG requires a single secure platform for the OIG workforce to access mission critical applications, thereby providing a secure, seamless user experience. Deploying a software platform, such as Okta, ensures only authorized OIG users can access its mission critical applications and subsequent data through multi-factor authentications, further safeguarding the OIG network and data.

Finally, as the OIG continues to expand its responsibilities and workforce to execute its mission needs, the number of IT assets connecting to the OIG's network has grown significantly. With this NAC software, the OIG can monitor, identify, control, and automatically mitigate the growing number of devices accessing the network, whether those devices are printers and scanners or large servers. The NAC will allow the OIG to improve its network security posture and better manage the growing IT assets needed to fulfill our mission.

(3) Modernize Current Cybersecurity Investigations Infrastructure – $1.5M

The OIG's Cyber Investigations Office (Cyber) continues to conduct comprehensive computer and mobile device forensic examinations for over 550 pieces of digital evidence annually, which includes computers, hard drives, cell phones, tablets, and other electronic media. These examinations support over 100 OIG investigations each year. Cyber Special Agents continue to investigate cyber-crime and insider threat matters, as well as attempted intrusions into the Department's network, spoofing of Department emails to accomplish criminal activity, and impersonation of Department officials in furtherance of fraud schemes. As the OIG's national security-related oversight activities and complexities of its investigations increase, the need for timely forensic examinations of digital evidence continues to grow. Specifically, the number of digital evidence items examined by the OIG's Cyber Investigations Office increased from 272 items in FY 2018 to 349 items in FY 2019, 564 items in FY 2020, and as of March 2021, approximately 300 items have been examined during FY 2021. In the interests of keeping pace with increasing demands, the OIG needs to modernize the current Cybersecurity Investigations Infrastructure. This program enhancement will allow the OIG to replace the digital forensic examination management system and build a forensic virtualization platform. The OIG will use new case management software to phase out the existing, foreign-owned, end-of-life system and track all exam requests and assignments to Cyber staff, capture key elements of the digital forensic exam process from cradle to grave, and document the digital forensic exams in accordance with CIGIE Quality Standards for Digital Forensics. Additionally, standing-up a secure virtual platform allows Cyber examiners, around the country, to process digital evidence in a more streamlined processing approach creating efficiencies to meet increasing case demands.

3. Current State and Impact on Performance

Without the enhancements noted above, the OIG would not be optimally positioned to meet rising cybersecurity demands on the IT infrastructure, remain agile enough to respond to threats like ransomware attacks, or maintain the IT enhancement pace set by the DOJ. Specifically, direct impacts include the OIG's inability to continue hardening the organization's enterprise IT environment against persistent and increasingly complex security threats. Also, the OIG risks

creating a large technical gap between the DOJ's and OIG's IT infrastructures and impacting its ability to comprehensively support the OIG's growing mission needs in the areas of cybersecurity and cybersecurity investigations.

Funding
Information Technology (IT Enhancement)
(Dollars in Thousands)

Base Funding

FY 2021 Enacted				FY 2022 President's Budget				FY 2023 Current Services			
Pos	Agt/Atty	FTE	$(000)	Pos	Agt/Atty	FTE	$(000)	Pos	Agt/Atty	FTE	$(000)
26	0/0	26	$15,352.5	29	0/0/	29	$14,542.0	29	0/0	29	$12,578.1

Personnel Increase Cost Summary

Type of Position/Series	Modular cost per Position ($000)	1st Year Annualization	Number of FTE's Requested	FY 2023 Requested ($000)	FY 2024 Net Annualization (change from 2023)($000)	FY 2025 Net Annualization (change from 2024)($000)
N/A						
Total Personnel						

Non-Personnel Costs

Non-Personnel Item	FY 2023 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2024 (Net change from 2023)	FY 2025 (Net change from 2024)
Modernizing IT Infrastructure	$1,771.0	N/A	1	$0.0	$0.0
Enhancing Security Footprint	$355.0	N/A	1	$0.0	$0.0
Cubersecurity Infrastructure	$1,500.0	N/A	1	$0.0	$0.0
Total Non-Personnel	**$3,626.0**	**N/A**	**1**	**$0.0**	**$0.0**

Total Request for this Item

	POS	Agt/Atty	FTE	Personnel ($000)	Non-Personnel ($000)	FY 2023 Total ($000)	FY 2024 Net Annualizations (change from 2023)($000)	FY 2025 Net Annualizations (change from 2024)($000)
Current Services	29	0/0	29	$5,886.4	$6,691.7	$12,578.1	N/A	N/A
Increases	0	0/0	0	$0.0	$3,626.0	$3,626.0	$0.0	$0.0
Grand Total	**29**	**0/0**	**29**	**$5,886.4**	**$10,317.7**	**$16,204.1**	**$0.0**	**$0.0**

B. Item Name: Office of Data Analytics Enhancement				
Strategic Goal(s) & Objective(s):	DOJ Strategic Plan Goal #1: Uphold The Rule Of Law. Objective 1.2 Promote Good Government			
Organizational Program:	OIG			
Program Increase:	Positions 0	Agt/Atty 0/0	FTE 0	Dollars $0
	Equipment/software/services:			Dollars $1,200,000
Total Request of Increase:	$1,200,000			

1. Description of Item

The OIG established the Office of Data Analytics (ODA) to lead the effort within the OIG to proactively gather and analyze large datasets in support of OIG oversight operations and its leadership. The OIG Data Analytics Program has proven essential in evaluating risk and identifying fraud, waste, and abuse in contracts, grants, healthcare costs, and government charge card transactions. Further, the Program has increased the OIG's ability to process information more efficiently and to more clearly articulate complex results for DOJ leadership and other stakeholders to use in making important decisions. The OIG is requesting a program increase of $1.2 million to support the OIG's Data Analytics Program. Specifically, the OIG is requesting a program increase of $220K to support the expansion of the IT security infrastructure, $250K for software licensing to provide a staging environment for two of the ODA's most critical data processing tools, $455K to develop and implement self-service capacity and functionality, and $275K for installation of enterprise-wide data visualization platform.

2. Justification

The OIG requires the requested enhancements for its burgeoning Data Analytics Program to (1) ensure the OIG Data Analytics System (ODAS) operates with minimal risk to its continuity of operation, employs all required and essential security to protect its highly sensitive data, and correctly stages data and analytics programs for use in its production environment; and (2) expand the availability and use of the Program's tools and resources, thereby exponentially increasing the positive impact the OIG has on Department operations.

(1) Further Modernize the IT Infrastructure

The field of data analytics has grown over the years with the move to Open Data within the Federal Government. For example, with the passing of the DATA Act and the GREAT Act, contracts and grants data are becoming more comprehensive and standardized, offering new and innovative ways to look at data. The need for data analytics requires a technologically advanced

and secure system to process large amounts of data obtained from the Department components and open sources.

Enhance Cybersecurity - $220K

As a result of the SolarWinds and FireEye security incidents the DOJ Office of the Chief Information Officer implemented a temporary Microsoft Azure Advance Persistent Threat solution. This solution monitors user behaviors within the cloud environment. However, ODAS currently remains an on-premise environment, and the OIG plans for ODAS to remain at least a hybrid cloud and on-premise system for the foreseeable future (funds permitting). Therefore, ODAS presently is not running a cybersecurity user behavior analytics monitoring tool to detect certain threats that are mitigated by the Microsoft Azure solution for cloud-based systems. In order to defend against insider threat, it's critical for the OIG to procure and maintain a user behavior analytics module as well as expand other critical cybersecurity programs designed for an on-premise environment. This would require up-front costs for initial licensing and professional services for installation and configuration, as well as include ongoing costs for annual subscription licensing.

Make Critical Improvements to ODAS Staging Environment - $250K

The OIG's Office of Data Analytics uses advanced data analytics tools and ETL (Extract, Transform, and Load) tools, which are highly critical to the successes of the Program. Currently, the OIG operates its tools in a test and production environment. While the test environment is important to experimenting with system tools and data prior to moving them into the live production environment, a staging environment is equally critical for ensuring that analytics programs, data manipulations, and IT component changes work in a staging environment prior to deploying them in the production environment.

1. Implement Enhancements to Increase System Availability and OIG Impact

Increase OIG Impact through Self-Service Analytics Access and Tools -$455K

Currently, ODAS can handle 80 users. In light of its increasing data repository and advances in its tools, the OIG Data Analytics Program has reached a pivotal moment in its evolution where developing and implementing a self-service functionality would ultimately enable ODAS to handle upwards of 500 users. This will require significant resources to develop and scale this functionality to effectively meet the needs of the OIG while continuing to prioritize the security of the data. The expected results of a self-service functionality will be the OIG delivering insights and recommendations in an even greater and quicker fashion than it does today. In addition, the OIG ODA is requesting to procure software resources for the OIG Data Analytics System to expand Virtual Desktop Interface (VDI) capacity and availability in the on-premise and cloud environments. This is essential to ensuring High VDI Availability to support audits and investigations. The software will enable more efficient use of resources so that users have continued access to the system, as well as increase the capacity for users.

Implement Enterprise-wide Data Visualization Platform - $275K

Over the last year the OIG began applying geospatial analytics software in its operations, and for several years has used an advanced visualization tool to illustrate and express complex results in

a more intuitive fashion. As the Department attempted to handle the effects of the COVID-19 pandemic on its operations, the OIG's analytics and visualization tools proved to be extremely valuable in providing Department leadership and other stakeholders with information they could easily understand and use in important policy and operational decisions. This included the OIG's development of several mobile-friendly, interactive dashboards as part of its COVID-19 and CARES Act oversight work. For example, the OIG's Office of Data Analytics worked with OIG inspectors, auditors, and attorneys in developing highly informative, interactive visuals and statistical dashboards illustrating the COVID-19 situation in all of the correctional facilities managed by the Federal Bureau of Prisons. The interest in and impact of this platform has been enormous, including these dashboards receiving over 10,000 hits and officials using this data to help inform early release decisions for certain inmates. In addition, the OIG published interactive results of an OIG survey on the Effects of COVID-19 on ATF, DEA, FBI, USAO, and USMS Investigative Operations, which had received over 7,000 hits as of April 2021. The OIG also developed dynamic web timelines to explain key events in the Department's CARES Act Spending, and more recently for the OIG's the Review of the Department of Justice's Planning and Implementation of Its Zero Tolerance Policy. These initial forays into more complex and innovative infographics and visualizations have allowed the OIG to communicate issues more effectively to the public and reach more stakeholders with easily consumable information. This change in how the public consumes information is part of a larger shift that an OIG must make to remain relevant and effective in today's world.

ODA has achieved the OIG's recent data visualization successes by working on one-off special projects and repurposing software to perform tasks that the software was not necessarily designed to do. For example, the OIG used geospatial software to create a mobile-friendly data visualization of survey results even though the public product did not include any maps. While ODA is circumventing some of the challenges associated with using tools for unintended purposes, the software does not currently include the full suite of options that is normally included in data visualization software. If the OIG does not invest in additional software, the OIG may not be able to use the recommended data visualization technique that would be most effective in communicating complex information to users. Additionally, since these public products have been one-off special projects, the OIG has not implemented the outreach and business processes to scale these activities. Thus, there are likely OIG audit, evaluation, investigative, and review public reports that could have incorporated interactive data features in the released public product. However, the report teams did not receive the required guidance and training on how to accomplish this task. The OIG has demonstrated the proof-of-concept of innovative data visualizations through specific special projects, but the OIG will need to invest in new tools to incorporate into the OIG normal report writing processes.

3. Current State and Impact on Performance

The IT infrastructure has grown since the OIG Data Analytics System was created in 2015, but there still is a great deal of work to do to expand the user base and ensure the stability of the system. The IT system houses critical hardware and software that allows the analysts to perform complex data analytics and ensure the security and integrity of the data we receive from components and open sources. As the office grows, so does the number of ongoing projects to accommodate the ever-increasing demand for our services, thereby increasing the datasets and the hardware and software capabilities required to securely store and analyze the data. The increase in datasets in our data repository requires significant increase in data management tools and practices.

Because there is an increase in data becoming available, the OIG's Office of Data Analytics struggles to meet the growing demand for its specialized services. Additionally, as more data becomes available, the OIG also must ensure that our IT infrastructure can handle the cybersecurity and storage of the data. Security is a top priority for the OIG and ensuring that the data is housed in an environment that mitigates risk of data breach and exposure requires significant resources to build and manage effectively on a day-to-day basis. In order to meet the growing needs of the OIG Divisions, we must ensure that the data analytics system be available for as many users as needed, that cyber-security of the system is monitored, and that data analytics tools we use are properly configured. It's also necessary to ensure that the environment remains stable so that it can handle the growing number of OIG users, such as OIG auditors, investigators, and evaluators.

DOJ OIG prides itself on being a leader within the oversight community by offering innovative ways to engage readers on our oversight findings and, when possible, put more data in the hands of Department leadership, our stakeholders, and the public. In FY 2020, the OIG published over 80 public products, and many included static graphics and tables to convey the impact of findings or clarify analysis. Investments in a public-facing data visualization platform will strengthen the OIG's ability to communicate audit, evaluation, inspection, and review findings to the public, and this greater level of accessibility and transparency will enhance the OIG's mission to keep those accountable who engage in waste, fraud, abuse, and misconduct in Department programs.

Funding
Office of Data Analytics Staff Enhancement
(Dollars in Thousands)

Base Funding

FY 2021 Enacted				FY 2022 President's Budget				FY 2023 Current Services			
Pos	Agt/Atty	FTE	$(000)	Pos	Agt/Atty	FTE	$(000)	Pos	Agt/Atty	FTE	$(000)
0	0	0	$4,635.8	0	0	0	$5,167.7	0	0	0	$5,600.7

Personnel Increase Cost Summary

Type of Position/Series	Modular cost per Position ($000)	1st Year Annualization	Number of FTE's Requested	FY 2023 Requested ($000)	FY 2024 Net Annualization (change from 2023)($000)	FY 2025 Net Annualization (change from 2024)($000)
N/A						
Total Personnel						

Non-Personnel Costs

Non-Personnel Item	FY 2023 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2024 (Net change from 2023)	FY 2025 (Net change from 2024)
ODA Enhancement	$1,200.0	N/A	1	($494.0)	$14.0
Total Non-Personnel	**$1,200.0**	**N/A**	**1**	**($494.0)**	**$14.0**

Total Request for this Item

	POS	Agt/Atty	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2024 Net Annualizations (change from 2023)($000)	FY 2025 Net Annualizations (change from 2024)($000)
Current Services	0	0/0	0	$3,823.1	$1,777.6	$5,600.7	N/A	N/A
Increases	0	0/0	0	$0.0	$1,200.0	$1,200.0	($494.0)	$14.0
Grand Total	**0**	**0/0**	**0**	**$3,823.1**	**$2,977.6**	**$6,800.7**	**($494.0)**	**$14.0**

C. Item Name: Cyber Forensics, Data Analytics, Special Reviews, and Operation Enhancement

Strategic Goal(s) & Objective(s):	DOJ Strategic Plan Goal #1: Uphold The Rule Of Law. Objective 1.2 Promote Good Government			
Organizational Program:	OIG			
Program Increase:	Positions 21	Agt/Atty 0/15	FTE 21	Dollars $3,950,000
	Equipment/software/services:		Dollars $0	
Total Request of Increase:	$3,950,000			

1. Description of Item

The Department of Justice (DOJ) Office of the Inspector General (OIG) requests 21 positions to support its effort in overseeing emerging and high-risk areas in which the Department must operate optimally to ensure the security of the nation and sound stewardship of American taxpayer dollars. The OIG conducted an extensive workforce analysis during FY 2021. The analysis determined that while we had the ceiling capacity, we did not have sufficient funding to hire to the authorized position levels. As a result of the analysis, we requested additional funding in FY 2022, but did not request an increase to the authorized position ceiling.

In FY 2022, the budget request is $127.1M, of which $3.9M are non-recurring costs. In FY 2023, we are requesting to maintain our top line of $127.1M and repurpose the $3.9M non-recurring costs to hire 21 additional positions in FY 2023 to support critical initiatives. These initiatives include the Department's (1) focus on addressing fraud involving over $5 trillion in pandemic-related funding, (2) ability to mitigate the exponentially increasing threat from domestic violent extremists (DVEs), and (3) security of its IT infrastructure from breach and compromise, and (4) effective and appropriate use of artificial intelligence. In addition, the positions will support increased digital forensic examination and eDiscovery workload, increased national-security and investigative workload, and requirements arising from the Body Worn Camera (BWC) Program.

Separately, OIG was at capacity to hire attorneys at the close of FY 2021. As such, in FY 2022 during the spend plan cycle, we plan to request the reallocation of 7-10 attorney positions within our authorized position ceiling. For FY 2023, we request an additional 4 attorney positions. These 4 positions will be part of the request to increase our ceiling for FY 2023, and part of the total 21 position request.

The descriptions below underscore the accomplishments that we have achieved and their significant impacts on the efficiencies and effectiveness of the Department's programs and operations. However, due to the substantial requests for increased transparency and accountability in the critical areas of audit, data analysis, cyber forensics, investigations, evaluations, and special reviews, the additional 21 positions will address our need for having the requisite level of experience and staff to perform these critical functions. Our ask is predicated on a comprehensive review of workforce needs to meet our enhanced oversight requirements.

2. Justification

Audit Oversight

Since March 6, 2020, Congress has passed six pieces of legislation totaling over $5.4 trillion to respond to the Coronavirus. It is the responsibility of the DOJ to lead investigations and prosecutions of pandemic-related fraud, and it is the duty of DOJ's OIG to ensure DOJ is operating optimally in these areas. Criminals continue to exploit pandemic-related funding worldwide through a variety of scams, including, but not limited to: (1) selling fake cures or vaccines; (2) phishing emails; (3) malicious websites; (4) seeking donations to illegitimate or non-existent charitable organizations; and (5) emails, texts, or robocalls asking for social security, banking, or credit card numbers to receive a vaccine. The OIG also issued a fraud alert advising DOJ procurement executives of emerging risks pertaining to pandemic-related purchases and continues to assess incoming pandemic-fraud allegations. The OIG also initiated an audit to examine the Criminal Division's and the Executive Office of the U.S. Attorneys' management and coordination of pandemic-related fraud allegations and referrals. Beginning in early March 2020, the OIG shifted a significant portion of its oversight efforts toward assessing DOJ's pandemic response.

The OIG has completed numerous impactful reviews including oversight of $850 million received by DOJ's Office of Justice Programs, and the preparedness and responsiveness of U.S. Prison facilities where, as of September 2021, 252 federal inmates and 6 staff have died of COVID-19. However, as pandemic-related funding has grown, the OIG remains responsible for the oversight of numerous other components and programs. This important work requires additional resources to ensure effective oversight, including the onboarding of additional auditors and data scientists. With additional resources, the OIG can continue to enhance our innovative COVID-19 dashboards and ensure that our oversight will continue to meet the expectations of Congress and the public in deterring waste, fraud, and abuse.

In June 2021, the White House released the National Strategy for Countering Domestic Terrorism, which notes that domestic terrorism has evolved into the most urgent terrorism threat the United States faces today. Central to this strategy is the Department of Justice's role in identifying, investigating, and prosecuting DVEs. According to Attorney General Merrick Garland, DOJ must: (i) understand and share information regarding the full range of threats; (ii) prevent domestic terrorists from successfully recruiting, inciting, and mobilizing Americans to violence; (iii) redouble and expand our efforts to deter and disrupt domestic terrorism activity before it yields violence; and (iv) address the long-term issues that contribute to domestic terrorism in our country. The OIG recognizes the importance of the Department's ability to address the DVE threat, and in September 2021 initiated an audit to evaluate the Department's efforts to develop and effectively implement its strategy to address the DVE threat. While we

believe any findings related to this audit will help inform Department leadership of concerns related to its new strategy to mitigate the DVE threat, in order to maintain robust oversight of the Department's expanded effort to address this ever-evolving threat, the OIG requires additional staff with expertise in national security, civil liberties, classified systems, insider threats, data analytics, and strategy evaluation. Additional OIG resources not only correspond to the increase in DOJ funding requested for FY 2022 but will allow the OIG to more effectively share and leverage information learned to initiate follow-up audits and reviews associated with emerging DVE risks and related DOJ strategy shifts.

The 2021 SolarWinds breach was one of the most widespread and sophisticated hacking campaigns ever conducted against the federal government and private sector. The Department said the Advanced Persistent Threat (APT) group responsible for the SolarWinds breach had access to all email communications and attachments found within the Department's compromised Microsoft Office 365 accounts for nearly 8 months. The ever-changing landscape of cyber intrusions, the state sponsorship of those intrusions, and the sensitive information contained in both the Department's unclassified and classified IT systems make it vital that the OIG be able to oversee Department efforts to secure its data and its IT systems. To accomplish this critical oversight, the OIG needs personnel with IT security backgrounds and experience, enabling the OIG to more effectively oversee the Department's practices for securing its systems and data. With these additional resources, the OIG will increase its audits and assessments of the Department's efforts to thwart and mitigate the effects of inevitable future attacks, similar in magnitude to SolarWinds. While the OIG performs statutorily required FISMA work, the focus of these positions would include both the DOJ's overall implementation of security efforts, as well as the role the DOJ has in dealing with such security issues through its national security, investigative, and prosecutorial roles.

The use of AI technology (e.g., facial recognition) has the potential to amplify existing concerns related to civil liberties, ethics, and social disparities because AI systems are created using data that may reflect preexisting biases or social inequities. AI stakeholders must ensure that the AI system uses data sets appropriate for the problem, selects the most suitable algorithms, and evaluates and validates that the system is functioning as intended. Without such assurances, the use of AI technologies may result in unintended consequences. As of FY 2020, the Department owns seven facial recognition systems and accesses four systems owned by other federal agencies, and uses these systems for domestic law enforcement, physical security, national security and defense, video management, and educational purposes. Given the number of facial recognition technology systems currently in use by Department components and the Department's goal of accelerating usage of this technology, it is vital that the Department employ personnel who have skills and experience with designing, developing, assessing, and monitoring AI systems. Equally important, the OIG needs to recruit and retain personnel with AI expertise in order to understand the challenges with AI systems to perform comprehensive oversight of this emerging technology. The additional OIG staff would enhance the OIG's ability to conduct OIG oversight audits and reviews in the area of AI to ensure these systems and programs are functioning as intended and adding value and efficiencies to the Department's operations, while not creating unintended consequences related to civil liberties, ethics, or social disparities. Ultimately, the OIG's increased oversight of AI technology would provide Congress and the taxpayer critical, independent assessments of the DOJ's AI strategy, use, and results.

Each year, through grants, contracts, and other federal assistance, the Department awards tens of billions of dollars to state and local governments, non-profit entities, federal contractors, and

other organizations. It is critical for the Department to ensure that any recipient of its funds does not engage in discrimination given the Department's responsibility to ensure civil rights and given that certain laws prohibit discrimination for those receiving federal funds, such as the Civil Rights Act of 1964 and Safe Streets Act of 1968. In fact, in September 2021, the Associate Attorney General ordered an initiative to ensure the Department was doing enough to ensure recipients of Department grant funds were not engaging in discrimination. Each year, the OIG adds immense value in helping the Department improve its grant and contract practices. With additional personnel, the OIG can help the Department ensure it has the controls and practices to ensure the funds it awards to outside entities are not used to further the discrimination of American citizens.

Data Analytics

The Office of Data Analytics (ODA) assists all of the OIG by providing specialized support in statistical analysis and modeling, data visualizations, big data analysis, and general data processing. ODA fills a pressing need to augment the agency's work by providing data-driven analytics to bolster audit findings, identify potential investigative leads, and corroborate information provided in interviews of key personnel. Demand from each of the agency's divisions has increased, and in order to meet the agency's needs to supplement and strengthen its work through specialized data tools, modeling, and analysis, a commensurate increase in ODA resources is needed. Currently ODA staff supports numerous public-facing audit and inspection reports and innovative special projects (e.g., grant risk model), to help prioritize where the OIG conducts oversight. Ad-hoc analysis requests across the OIG doubled in FY 2020 alone.

The role of data analytics has expanded in recent years due the prevalence of available data from federal agencies. The ODA leverages its data analytics platform to meet an immediate need which provides weekly geolocation information on the number of COVID-19-related cases involving BOP employees and incarcerated individuals in Federal Bureau of Prisons facilities since the onset of the pandemic. This analysis has been crucial to informing the work performed by the OIG during a national crisis, as well as keeping the Department informed. This work is also available to the public to allow for greater transparency. In addition to the BOP interactive dashboard, ODA's data services have been increasingly used in OIG public products.

The growth in demand for data analytics and visual representations of large volumes of information will continue to grow in the OIG as this information lends itself for rapid decision making to address existing and emerging mission needs across the OIG and the DOJ.

Cyber Forensics and Investigation

Due to continued increases in volume for both digital forensic exam requests and eDiscovery requests, the current OIG Cyber Investigations Office (Cyber) workforce cannot maintain the same level of mission support without augmenting its staff. Cyber continues to conduct comprehensive computer and mobile device forensic examinations for over 600 pieces of digital evidence annually, which includes computers, hard drives, cell phones, tablets, and other electronic media. These examinations support over 100 OIG investigations each year, as well as reviews conducted by the OIG's Oversight & Review Division. With the OIG's increased national security-related oversight activities and the complexities of its investigations, the need for timely forensic examinations of digital evidence continues to grow. Specifically, the number of digital evidence items examined by Cyber steadily increased from 272 items in FY 2018 to

349 items in FY 2019, 564 items in FY 2020 and as of mid-September 2021, approximately 611 items have been examined during FY 2021. In addition, Cyber has handled 25 eDiscovery requests for the OIG thus far in FY 2021, involving substantial data collections for dozens of custodians. These requests require Cyber examiners to filter, sort, and produce electronic records pertaining to civil matters, internal matters, discovery for criminal cases and FOIA requests. These eDiscovery requests also required over 60 instances where a Cyber examiner needed to upload an eDiscovery production into the Relativity Review Platform for Agent or Attorney review.

OIG is requesting additional Digital Investigative Analyst positions in order to maintain pace with the increasing digital forensic examination workload and research and test decryption solutions, while providing detailed analysis of data recovered from digital evidence. These positions will also help Cyber maintain its critically important level of support for the increased frequency and volume of eDiscovery requests. OIG currently has six funded Examiner positions but one of the positions had to be converted to a Lab Manager in order to oversee quality assurance, policy, SOPs and conduct on-site inspections at six digital forensic lab locations across the country. As a result of these responsibilities, the Lab Manager is unable to maintain a full exam load due to the additional duties of the position. Furthermore, OIG Digital Investigative Analysts (examiners) routinely encounter encryption when attempting to lawfully access digital evidence. OIG has purchased law enforcement tools, to include two devices with a combined license fee of approximately $100,000 per year. These tools require Cyber examiners to undergo specialized training and certifications. OIG has also trained an examiner to conduct specialized circuit board soldering techniques to attempt bypassing passwords and encryption where OIG has lawful authority to access the data contained on the device.

OIG's Cyber Special Agents continue to investigate cyber-crime and insider threat matters, as well as spoofing of Department emails to accomplish criminal activity, impersonation of Department officials in furtherance of fraud schemes, and extortion attempts relating to DOJ investigations. OIG currently has six funded non-supervisory Cyber Special Agent positions that conduct a variety of investigations involving child exploitation crimes committed by DOJ employees or contractors, international fraud schemes, and cyber threats made against DOJ employees. For example, Cyber Agents conducted an international money laundering and bank fraud investigation where a DOJ employee pleaded guilty to conspiracy to make false statements to a bank and Agents seized over $73 million that was fraudulently brought into the U.S. banking industry by foreign actors. Of the $73 million seizure, $36.3 million was forfeited and the remaining amount is pending forfeiture.

Cyber Agents investigated an International Cyber fraud scheme where bad actors used the names, addresses, and phone numbers of government procurement officials, along with similarly named email addresses to trick U.S. businesses into shipping hundreds of thousands of dollars of IT hardware to the bad actors based on phony Purchase Orders. As a direct result of this investigation, OIG Cyber Agents seized over $1 million in stolen IT hardware before it left JFK airport and the individual who arrived to pick up a dummy shipment in Nigeria was arrested by a local task force. OIG Agents also investigate cyber threats sent to DOJ employees and in a recent matter located an individual responsible for sending a threatening email by tracing their Internet Protocol address through appropriate legal process.

In January 2020, OIG Cyber Agents arrested a DOJ employee in New York City who was subsequently charged with one count of attempted production of child pornography, one count of

attempted receipt of child pornography, and one count of attempted coercion and enticement of a minor. This DOJ employee was convicted at trial in June 2021.

Cyber Agents are also conducting investigations involving cyber stalking committed by a DOJ employee, and an investigation of a DOJ law enforcement agent who was present during the Capitol riot on January 6, 2021. OIG Cyber Agents also quickly identified an individual who was impersonating a Deputy U.S. Marshal and posting inflammatory and threatening content on the internet prior to the Presidential Inauguration. Additionally, Cyber Agents are concluding an investigation where numerous individuals conspired to utilize large drones to smuggle contraband into a Federal prison. In September 2021, one of the individuals was sentenced to 43 months for his role in the scheme.

In accordance with a Department Policy memo dated June 7, 2021, which requires the use of Body Worn Cameras (BWC) by DOJ Law Enforcement Agents, the OIG is poised to spend over $600,000 in the next five years to implement a body worn camera (BWC) program for OIG Agent use during enforcement operations. The BWC program falls under the Cyber Investigations Office (Cyber). Although a program manager was hired to oversee implementation of the program and function as the Contracting Officer's Representative, additional resources will be needed for the successful deployment and management of over 120 cameras, dozens of docking stations, software on each Agent laptop and BWC applications for Agent mobile devices. The Program manager will need the assistance of two specialists to successfully implement, maintain, and evolve the OIG's BWC program. The OIG's BWC program will also require storage management, archival processing, as well as redaction or blur of BWC videos when required for court or FOIA requests.

Investigative Support

With continual calls for law enforcement reform and accountability through various reporting channels, the Investigative Support Branch (ISB) is challenged with continually evolving to meet these needs with insufficient personnel resources. The ISB delivers and executes the most sensitive and unique programs in the Investigations Division. These programs include compliance with law and Council of the Inspectors General on Integrity and Efficiency (CIGIE) standards, ranging in scope from law enforcement equipment procurement and management and national program management, while pivoting to meet increasing reporting requirements such as the National Incident-Based Reporting System. From April through September 2021, ISB staff responded to more than 1,000 requests for assistance in varying complexity from assistance with database accounts to policy evolution and law enforcement program modifications, despite staffing shortages.

To keep pace with increasing demands, ISB must modernize and update its training, inspection, and law enforcement programs. Specifically, adding a program manager will enable redevelopment of the office review program to ensure CIGIE standards and applicable laws, rules, and regulations are followed, while modeling a gold standard for the OIG community. These enhancements will provide real-time management for field offices and ensure corrective actions for deficiencies are effected forthwith, while ensuring agency policy is timely updated. In addition, specialists will be positioned to provide proper oversight of law enforcement equipment, oversee associated contracts and procurements, and manage the OIG fleet program. Adding key personnel within ISB will ensure an appropriate level of response to OIG field offices while eliminating the overtime required to cover-down on these programs from other branches within the Division. Most importantly, additional staff will ensure adequate delivery of

compliance program and law enforcement equipment, as well as availability of resources, while ensuring judicious procurements and contracts are carried out.

3. Current State and Impact on Performance

Without the enhancements noted above, it will impede our ability to timely respond to and sufficiently address the increased demands for transparency and accountability. The impacts of not having the additional 21 positions will affect our ability to fully execute on the Department's goals and priorities, including: cyber security, cybercrime, combatting violent crime, fraud, waste, and abuse, misconduct, and other critical oversight functions. With the recent and significant increases for continued oversight from Congress and Department leadership, the OIG needs to be appropriately resourced to adequately and adeptly respond to these emerging requests.

Funding
Cyber Forensics, Data Analytics, Special Reviews and Operation Enhancement
(Dollars in Thousands)

Base Funding

FY2021 Enacted				FY2022 President's Budget				FY 2023 Current Services			
Pos	Agt/Atty	FTE	$0	Pos	Agt/Atty	FTE	$0	Pos	Agt / Atty	FTE	$0
491	146/35	466	$86,165	539	146/35	529	$99,812	539	146/35	529	$107,426

Personnel Increase Cost Summary

Type of Position/Series	Modular cost per Position ($000)	Number of FTE's Requested	FY 2023 Requested ($000)	FY 2024 Net Annualization (change from 2023)($000)	FY 2025 Net Annualization (change from 2024)($000)
Attorney (905)	$262	4	$1,048	($62)	$14
Accounting and Budget GS13 (500-599)	$182	3	$547	($46)	$8
Cyber Analysts (0300-0399)	$288	3	$863	($34)	$30
Analysts GS 14 (0300-0399)	$204	1	$204	($15)	$6
Analysts GS15 (0300-0399)	$235	1	$235	($15)	$7
Analysts GS12 (0300-0399)	$153	4	$614	($62)	$16
Analysts GS07 (0300-0399)	$99	1	$99	($15)	$3
Analysts GS 05 (0300-0399)	$85	4	$340	($62)	$8
Total Personnel	**$1,509**	**21**	**$3,950**	**($312)**	**$91**

Total Request for this Item

	POS	Agt/Atty/Other	Non-Personnel ($000)	Total ($000)	FY 2024 Net Annualization (change from 2023)($000)	FY 2025 Net Annualization (change from 2024)($000)
Current Services	539	146/35/358	$0.0	$107,426	N/A	N/A
Increases	21	0/15/21	$0.0	$3,950	($312)	$91
Grand Total	**560**	**146/50/379**	**$0.0**	**$111,376**	**($312)**	**$91**

VII. Appendix

A. Statistical Highlights

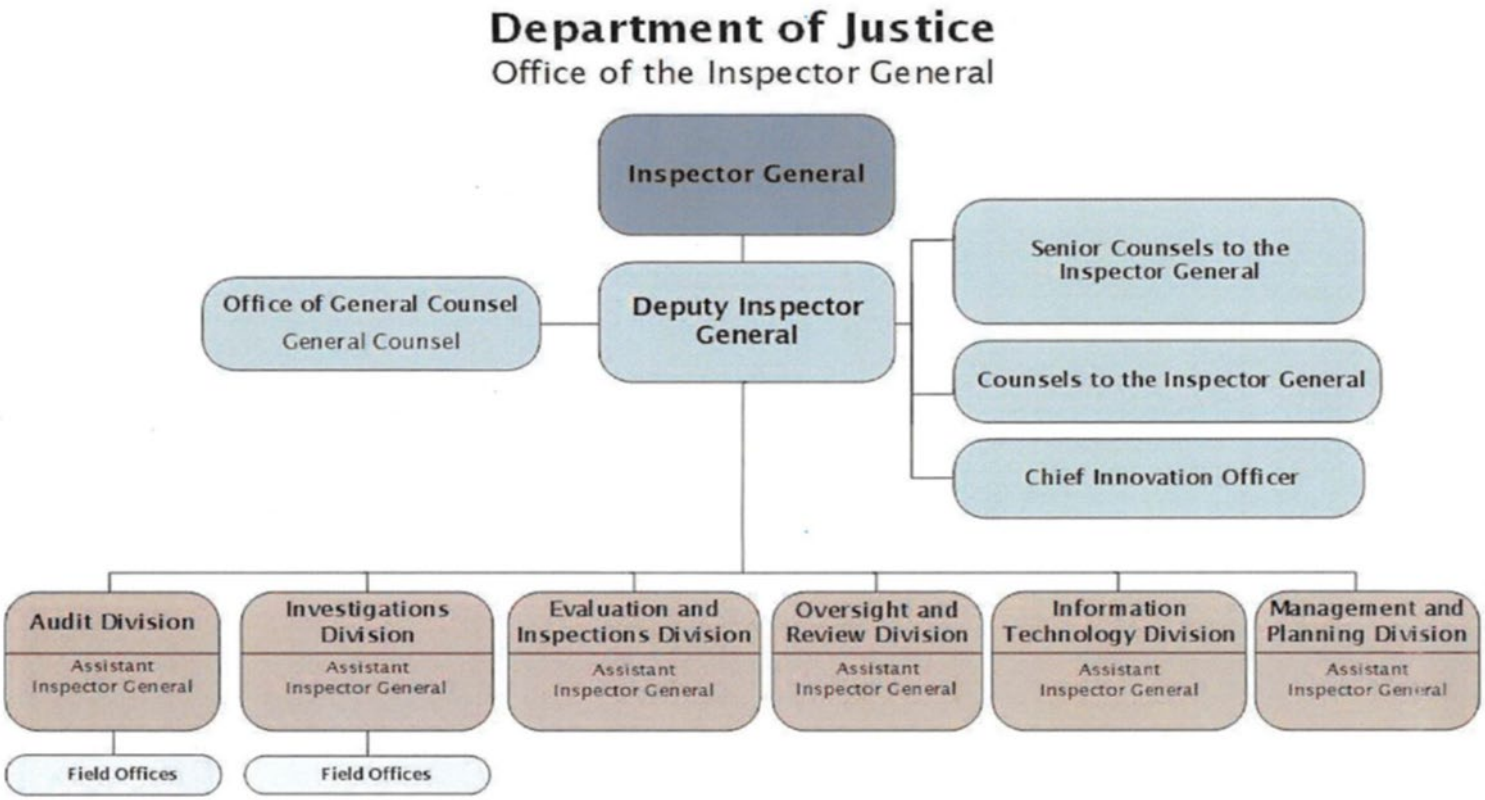
April 1, 2021–September 30, 2021

The following table summarizes the OIG activities discussed in our most recent *Semiannual Report to Congress.* As these statistics and the following highlights illustrate, the OIG continues to conduct wide-ranging oversight of Department programs and operations.

April 1, 2021 - September 30, 2021		
Allegations Received by the Investigations Division		6,345
Investigations Opened		137
Investigations Closed		143
Arrests		52
Indictments/Information		59
Convictions/Pleas		68
Administrative Actions		66
Monetary Recoveries	$	4,910,911
Audit Reports Issued		41
Questioned Costs	$	5,697,917
Recommendations for Management Improvements		302
Single Audit Act Reports Issued		12
Questioned Costs	$	181,914
Recommendations for Management Improvements		25

VIII. Exhibits

A. Organizational Chart



Approved by: Michael E. Horowitz
Inspector General

Date: 2/11/19

B. 1. Summary of Requirements

Summary of Requirements
Office of the Inspector General
Salaries and Expenses
(Dollars in Thousands)

	FY 2023 Request		
	Positions	**Estimate FTE**	**Amount**
2021 Enacted 1/	**491**	**466**	**120,565**
Total 2021 Enacted	**491**	**466**	**120,565**
2022 Continuing Resolution	**491**	**466**	**120,565**
Expected Change from FY 2022 CR	48	63	16,619
Total 2022 President's Budget	**539**	**529**	**137,184**
Technical Adjustments			
Non-Recurral - Oversight and Auditing - From CVF	0	0	-10,000
Total Technical Adjustments	**0**	**0**	**-10,000**
Base Adjustments			
Transfers:			
Transfers - Oversight and Auditing - From CVF	0	0	10,000
Pay and Benefits	0	0	3,375
Domestic Rent and Facilities	0	0	471
Non-Personnel Related Annualizations	0	0	-3,950
Total Base Adjustments	**0**	**0**	**9,896**
Total Technical and Base Adjustments	**0**	**0**	**-104**
2023 Current Services	**539**	**529**	**137,080**
Program Changes			
Increases:			
Information Technology Enhancement	0	0	3,626
Office of Data Analytics Enhancement	0	0	1,200
Cyber Forensics, Data Analytics, Special Reviews, and Operations Enhancement	21	21	3,950
Subtotal, Increases	21	21	8,776
Total Program Changes	**21**	**21**	**8,776**
2023 Total Request	**560**	**550**	**145,856**
2022 - 2023 Total Change	21	21	8,672

1/ FY 2021 FTE is actual

B. 2. Summary of Requirements by Decision Unit

Summary of Requirements
Office of the Inspector General
Salaries and Expenses
(Dollars in Thousands)

Program Activity	FY 2021 Enacted			FY 2022 President's Budget			FY 2023 Technical and Base Adjustments			FY 2023 Current Services		
	Positions	Actual FTE	Amount	Positions	Est. FTE	Amount	Positions	Est. FTE	Amount	Positions	Est. FTE	Amount
OIG Audits, Inspections, Investigations, and Reviews	491	466	120,565	539	529	137,184	0	0	-104	539	529	137,080
Total Direct	**491**	**466**	**120,565**	**539**	**529**	**137,184**	**0**	**0**	**-104**	**539**	**529**	**137,080**
Balance Rescission			0			0			0			0
Total Direct with Rescission			**120,565**			**137,184**			**-104**			**137,080**
Reimbursable FTE		68			20			0			20	
Total Direct and Reimb. FTE		**534**			**549**			**0**			**549**	
Other FTE:												
LEAP		0			0			0			0	
Overtime		0			0			0			0	
Grand Total, FTE		**534**			**549**			**0**			**549**	
Sub-Allotments and Direct Collections FTE		*5*			*5*			*0*			*5*	

Program Activity	2023 Increases			2023 Offsets			2023 Request		
	Positions	Est. FTE	Amount	Positions	Est. FTE	Amount	Positions	Est. FTE	Amount
OIG Audits, Inspections, Investigations, and Reviews	21	21	8,776	0	0	0	560	550	145,856
Total Direct	**21**	**21**	**8,776**	**0**	**0**	**0**	**560**	**550**	**145,856**
Balance Rescission			0			0			0
Total Direct with Rescission			**8,776**			**0**			**145,856**
Reimbursable FTE		0			0			20	
Total Direct and Reimb. FTE		**21**			**0**			**570**	
Other FTE:									
LEAP		0			0			0	
Overtime		0			0			0	
Grand Total, FTE		**21**			**0**			**570**	
Sub-Allotments and Direct Collections FTE		*0*			*0*			*5*	

C. Summary of Requirements by Decision Unit

FY 2023 Program Increases/Offsets by Decision Unit

Office of the Inspector General

Salaries and Expenses

(Dollars in Thousands)

Program Increases	Location of Description by Program Activity	OIG Audits, Inspections, Investigations, and Reviews				Total Increases			
		Positions	Agt./Atty.	Est. FTE	Amount	Positions	Agt./Atty.	Est. FTE	Amount
Information Technology Enhancement		0	0	0	3,626	0	0	0	3,626
Office of Data Analytics Enhancement		0	0	0	1,200	0	0	0	1,200
Cyber Forensics, Data Analytics, Special Reviews, and Operations Enhancement		21	4	21	3,950	21	4	21	3,950
Total Program Increases		**21**	**4**	**21**	**8,776**	**21**	**4**	**21**	**8,776**

Program Offsets	Location of Description by Program Activity	OIG Audits, Inspections, Investigations, and Reviews				Total Offsets			
		Positions	Agt./Atty.	Est. FTE	Amount	Positions	Agt./Atty.	Est. FTE	Amount
No Program Offsets									
Total Program Offsets									

D. Resources by DOJ Strategic Goal and Objective

Resources by Department of Justice Strategic Goal and Objective

Office of the Inspector General

Salaries and Expenses

(Dollars in Thousands)

Strategic Goal and Strategic Objective	FY 2021 Enacted			FY 2022 President's Budget		FY 2023 Current Services		FY 2023 Increases		FY 2023 Offsets		FY 2023 Total Request	
	Direct & Reimb FTE	*SubAllot/Dir Coll FTE*	Direct Amount	Direct & Reimb FTE	Direct Amount	Direct & Reimb FTE	Direct Amount	Direct & Reimb FTE	Direct Amount	Direct & Reimb FTE	Direct Amount	Direct & Reimb FTE	Direct Amount
Goal 1 Uphold the Rule of Law													
1.2 Promote Good Government	534	*5*	120,565	549	137,184	549	137,080	21	8,776	0	0	570	145,856
Subtotal, Goal 1	**534**	***5***	**120,565**	**549**	**137,184**	**549**	**137,080**	**21**	**8,776**	**0**	**0**	**570**	**145,856**
TOTAL	**534**	***5***	**120,565**	**549**	**137,184**	**549**	**137,080**	**21**	**8,776**	**0**	**0**	**570**	**145,856**

E. Justification for Technical and Base Adjustments

Justifications for Technical and Base Adjustments
Office of the Inspector General
Salaries and Expenses
(Dollars in Thousands)

		Positions	Estimate FTE	Amount
	Technical Adjustments			
1	Non-Recurral - Oversight and Auditing - From CVF Changing from $10M Remibursable Funding to a Transfer to Direct funding.	0	0	-10,000
	Subtotal, Technical Adjustments	**0**	**0**	**-10,000**
	Transfers			
1	Transfers - Oversight and Auditing - From CVF As of FY 2020, CVF funding is a direct transfer (vs. reimbursable).	0	0	10,000
	Subtotal, Transfers	**0**	**0**	**10,000**
	Pay and Benefits			
1	2023 Pay Raise - 4.6% This request provides for a proposed 4.6 percent pay raise to be effective in January of 2023. The amount requested, $2,938,000, represents the pay amounts for 3/4 of the fiscal year plus appropriate benefits ($1,880,000 for pay and $1,058,000 for benefits.)	0	0	2,938
2	Annualization of 2021 Approved Positions Personnel: This provides for the annualization of 9 new positions appropriated in 2021. Annualization of new positions extends up to 3 years to provide entry level funding in the first year, with a 1 or 2-year progression to a journeyman level. For 2021 increases, this request includes an increase of $53,000 for full-year payroll costs associated with these additional positions. Non-Personnel: This request includes a decrease of $132,300 for one-time items associated with the new positions, for a net of +/-$53,000.	0	0	53
3	Annualization of 2022 Pay Raise This pay annualization represents first quarter amounts (October through December) of the 2022 pay increase of 2.7%. The amount requested, $602,000, represents the pay amounts for 1/4 of the fiscal year plus appropriate benefits ($385,280 for pay and $216,720 for benefits.)	0	0	602
4	Changes in Compensable Days The decreased cost for one compensable day in FY 2023 compared to FY 2022 is calculated by dividing the FY 2021 estimated personnel compensation by 260 compensable days.	0	0	-306
5	Employees Compensation Fund The -$5,000 request reflects anticipated changes in payments to the Department of Labor for injury benefits under the Federal Employee Compensation Act.	0	0	-5
6	Health Insurance Effective January 2023, the component's contribution to Federal employees' health insurance increases by 2 percent. Applied against the 2022 estimate of $4,214,000, the additional amount required is $86,000.	0	0	86
7	Non-SES Awards This request provides a 1% non SES-Award increase to be effective in January of 2023. The amount requested $14,000 represents 1% of the FY 2023 Pay Raise for 3/4 of the fiscal year.	0	0	14
8	Retirement - CSRS to FERS Conversion Agency retirement contributions increase as employees under CSRS retire and are replaced by FERS employees. Based on U.S. Department of Justice Agency estimates, we project that the DOJ workforce will convert from CSRS to FERS at a rate of 0.8 percent per year, for both LEO and Non-LEO, based on the past 5 years of DOJ retirement data. The requested increase of $2,000 is necessary to meet our increased retirement obligations as a result of this conversion.	0	0	2
9	Retirement - FERS/FRAE Conversion Savings Agency retirement contributions will decrease as new FERS RAE employees are hired and replace CSRS and regular FERS employees. Based on OMB Circular A-11 FERS RAE withholding rates, we project agency savings from employees hired after December 31, 2012 of 1.8 percent of salaries for Non-LEO employees and 1.7 percent of salaries for LEO employees in FY 2022, for a savings of $9,000.	0	0	-9
	Subtotal, Pay and Benefits	**0**	**0**	**3,375**
	Domestic Rent and Facilities			
1	2CON Prospectus The -$471,000 request reflects anticipated changes in costs associated with FY 2022 leasehold improvements.	0	0	-471
2	Moves - Lease Expiration GSA requires all agencies to pay relocation costs associated with lease expirations. This request provides for the costs associated with new office relocations caused by the expiration of leases in FY 2023.	0	0	942
	Subtotal, Domestic Rent and Facilities	**0**	**0**	**471**
	Non-Personnel Related Annualizations			
1	Non-Recurral of FY 2022 Non-Personnel Items This ATB is for Non-Recurral of FY 2022 physical infrastructure ($2.950 million) enhancement and cloud funding ($1 million).	0	0	-3,950
	Subtotal, Non-Personnel Related Annualizations	**0**	**0**	**-3,950**
	TOTAL DIRECT TECHNICAL and BASE ADJUSTMENTS	**0**	**0**	**-104**

F. Crosswalk of 2021 Availability

Crosswalk of 2021 Availability

Office of the Inspector General
Salaries and Expenses
(Dollars in Thousands)

Program Activity	FY 2021 Enacted			Reprogramming/Transfers			Carryover	Recoveries/ Refunds	FY 2021 Availability		
	Positions	Actual FTE	Amount	Positions	Actual FTE	Amount	Amount	Amount	Positions	Actual FTE	Amount
OIG Audits, Inspections, Investigations, and Reviews	491	466	110,565	0	0	11,000	11,515	1,591	491	466	134,671
Total Direct	**491**	**466**	**110,565**	**0**	**0**	**11,000**	**11,515**	**1,591**	**491**	**466**	**134,671**
Balance Rescission			0			0	0	0			0
Total Direct with Rescission			110,565			11,000	11,515	1,591			134,671
Reimbursable FTE		68			0					68	
Total Direct and Reimb. FTE		534			0					534	
Other FTE:											
LEAP FTE		0			0					0	
Overtime		0			0					0	
Grand Total, FTE		534			0					534	
Sub-Allotments and Direct Collections FTE		*5*								*5*	

Reprogramming/Transfers:
$10,000K from Crime Victims Fund per PL 116-260
$1,000K from FY20 transferred in FY21 to 20/21 account
Carryover:
$10,000K from CVF Transfer
$186K from CARES Act Supplemental funding
$1,329K from Multi-Year 20/21 account
Recoveries/Refunds:
$200K - FY 20/21 HCFAC
$1,391K FY 21/22 HCFAC

G. Crosswalk of 2022 Availability

Crosswalk of 2022 Availability

Office of the Inspector General
Salaries and Expenses
(Dollars in Thousands)

Program Activity	FY 2022 President's Budget			Reprogramming/Transfers			Carryover	Recoveries/ Refunds	FY 2022 Availability		
	Positions	Est. FTE	Amount	Positions	Est. FTE	Amount	Amount	Amount	Positions	Est. FTE	Amount
OIG Audits, Inspections, Investigations, and Reviews	539	529	127,184	0	0	10,400	24,424	571	539	529	162,579
Total Direct	**539**	**529**	**127,184**	**0**	**0**	**10,400**	**24,424**	**571**	**539**	**529**	**162,579**
Balance Rescission			0			0	0	0			0
Total Direct with Rescission			127,184			10,400	24,424	571			162,579
Reimbursable FTE		20			0					20	
Total Direct and Reimb. FTE		549			0					549	
Other FTE:											
LEAP FTE		0			0					0	
Overtime		0			0					0	
Grand Total, FTE		549			0					549	
Sub-Allotments and Direct Collections FTE		*5*								*5*	

Reprogramming/Transfers:
$10,000K from Crime Victims Fund per PL 116-260
$400K from FY21 transferred in FY22 to FY 21/22 account
Carryover:
$20,023K from CVF Transfer
$1,095K FY 21/22 HCFAC
$3,300K FY 21/22 Multi Year
Recoveries/Refunds:
$571K FY 22/23 HCFAC Estimate

H.R. Summary of Reimbursable Resources

Summary of Reimbursable Resources

Office of the Inspector General
Salaries and Expenses
(Dollars in Thousands)

Collections by Source	2021 Actual			2022 Estimate			2023 Request			Increase/Decrease		
	Reimb. Pos.	Reimb. FTE	Amount	Reimb. Pos.	Reimb. FTE	Amount	Reimb. Pos.	Reimb. FTE	Amount	Reimb. Pos.	Reimb. FTE	Amount
Asset Forfeiture Fund	2	2	1,310	2	2	1,330	2	2	1,365	0	0	35
Council of the IGs on Integrity and Efficiency	1	1	100	1	1	100	1	1	150	0	0	50
Bureau of Alchohol, Tobacco, Firearms and Explosives	0	0	100	0	0	100	0	0	100	0	0	0
Working Capital Fund	7	7	2,592	7	6	2,692	7	6	2,756	0	0	64
Federal Bureau of Investigation	2	2	1,947	2	2	1,979	2	2	2,028	0	0	49
Federal Prison Industries	2	2	1,391	2	2	1,318	2	2	1,353	0	0	35
Federal Prison System	2	2	1,324	2	2	1,343	2	2	1,379	0	0	36
Offices, Boards, and Divisions	6	6	6,287	6	5	6,393	6	5	6,552	0	0	159
Crime Victim Fund	48	46	12,000	0	0	0	0	0	0	0	0	0
Budgetary Resources	**70**	**68**	**27,051**	**22**	**20**	**15,255**	**22**	**20**	**15,683**	**0**	**0**	**428**

Obligations by Program Activity	2021 Actual			2022 Estimate			2023 Request			Increase/Decrease		
	Reimb. Pos.	Reimb. FTE	Amount	Reimb. Pos.	Reimb. FTE	Amount	Reimb. Pos.	Reimb. FTE	Amount	Reimb. Pos.	Reimb. FTE	Amount
OIG Audits, Inspections, Investigations, and Reviews	70	68	27,051	22	20	15,255	22	20	15,683	0	0	428
Budgetary Resources	**70**	**68**	**27,051**	**22**	**20**	**15,255**	**22**	**20**	**15,683**	**0**	**0**	**428**

H.S. Summary of Sub-Allotments and Direct Collections Resources

Office of the Inspector General
Salaries and Expenses
(Dollars in Thousands)

Sub-Allotments and Direct Collections	2021 Actual			2022 Estimate			2023 Request			Increase/Decrease		
	SubAllot-Dir Coll Pos	SubAllot-Dir Coll FTE	Amount	SubAllot-Dir Coll Pos	SubAllot-Dir Coll FTE	Amount	SubAllot-Dir Coll Pos	SubAllot-Dir Coll FTE	Amount	SubAllot-Dir Coll Pos	SubAllot-Dir Coll FTE	Amount
HCFAC	5	5	1,666	5	5	1,666	5	5	1,666	0	0	0
Budgetary Resources	**5**	**5**	**1,666**	**5**	**5**	**1,666**	**5**	**5**	**1,666**	**0**	**0**	**0**

Obligations by Program Activity	2021Actual			2022 Estimate			2023 Request			Increase/Decrease		
	SubAllot-Dir Coll Pos	SubAllot-Dir Coll FTE	Amount	SubAllot-Dir Coll Pos	SubAllot-Dir Coll FTE	Amount	SubAllot-Dir Coll Pos	SubAllot-Dir Coll FTE	Amount	SubAllot-Dir Coll Pos	SubAllot-Dir Coll FTE	Amount
OIG Audits, Inspections, Investigations, and Reviews	5	5	1,666	5	5	1,666	5	5	1,666	0	0	0
Budgetary Resources	**5**	**5**	**1,666**	**5**	**5**	**1,666**	**5**	**5**	**1,666**	**0**	**0**	**0**

I. Detail of Permanent Positions by Category

Detail of Permanent Positions by Category

Office of the Inspector General

Salaries and Expenses

(Dollars in Thousands)

Category	FY 2021 Enacted			FY 2022 President's Budget			FY 2023 Request					
	Direct Pos.	Reimb. Pos.	*SubAllot-Dir Coll Pos.*	Direct Pos.	Reimb. Pos.	*SubAllot-Dir Coll Pos.*	ATBs	Program Increases	Program Offsets	Total Direct Pos.	Total Reimb. Pos.	*Total SubAllot-Dir Coll Pos*
Security Specialists (080)	4	0	*0*	4	0	*0*	0	0	0	4	0	*0*
Human Resources Management (0200-0260)	10	0	*0*	10	0	*0*	0	0	0	10	0	*0*
Clerical and Office Services (0300-0399)	157	26	*0*	157	4	*0*	-15	14	0	156	4	*0*
Accounting and Budget (500-599)	95	34	*0*	143	14	*0*	0	3	0	146	14	*0*
Attorneys (905)	35	0	*0*	35	0	*0*	15	4	0	54	0	*0*
Paralegal Specialist (0950)	2	0	*0*	2	0	*0*	0	0	0	2	0	*0*
Information & Arts (1000-1099)	4	0	*0*	4	0	*0*	0	0	0	4	0	*0*
Operations Research Analyst	1	1	*1*	1	0	*1*	0	0	0	1	0	*1*
Statistician (1530)	1	2	*0*	1	0	*0*	0	0	0	1	0	*0*
Inspection, Investigation, Enforcement Analyst(1801)	5	1	*1*	5	0	*1*	0	0	0	5	0	*1*
Misc.Inspectors/Investigative Assistants (1802)	6	0	*0*	6	0	*0*	0	0	0	6	0	*0*
Criminal Investigative Series (0082 & 1811)	146	2	*0*	146	0	*0*	0	0	0	146	0	*0*
Information Technology Mgmt (2210-2299)	25	4	*1*	25	4	*1*	0	0	0	25	4	*1*
General Investigation	0	0	*2*	0	0	*2*	0	0	0	0	0	*2*
Total	**491**	**70**	***5***	**539**	**22**	***5***	**0**	**21**	**0**	**560**	**22**	***5***
Headquarters Washington D.C.	216	70	*0*	216	22	*5*	0	21	0	237	22	*5*
US Fields	275	0	*0*	323	0	*0*	0	0	0	323	0	*0*
Foreign Field	0	0	*0*	0	0	*0*	0	0	0	0	0	*0*
Total	**491**	**70**	***0***	**539**	**22**	***5***	**0**	**21**	**0**	**560**	**22**	***5***

J. Financial Analysis of Program Changes

Financial Analysis of Program Changes

Office of the Inspector General

Salaries and Expenses

(Dollars in Thousands)

Grades	OIG Audits, Inspections, Investigations, and Reviews				Total Program Changes	
	Program Increases		Program Decreases			
	Positions	Amount	Positions	Amount	Positions	Amount
GS-15	5	1,283	0	0	5	1,283
GS-14	1	204	0	0	1	204
GS-13	6	1,410	0	0	6	1,410
GS-12	4	614	0	0	4	614
GS-7	1	99	0	0	1	99
GS-5	4	340	0	0	4	340
Total Positions and Annual Amount	**21**	**3,950**	**0**	**0**	**21**	**3,950**
Lapse (-)	0	0	0	0	0	0
11.5 - Other personnel compensation		0		0		0
Total FTEs and Personnel Compensation	**21**	**3,950**	**0**	**0**	**21**	**3,950**
31.0 - Equipment		4,826		0		4,826
Total Program Change Requests	**21**	**8,776**	**0**	**0**	**21**	**8,776**

K. Summary of Requirements by Object Class

Summary of Requirements by Object Class
Office of the Inspector General
Salaries and Expenses
(Dollars in Thousands)

Object Class	FY 2021 Actual		FY 2022 President's Budget		FY 2023 Request		Increase/Decrease	
	Act. FTE	Amount	Direct FTE	Amount	Direct FTE	Amount	Direct FTE	Amount
11.1 - Full-time permanent	466	54,962	529	68,365	550	72,434	21	4,070
11.3 - Other than full-time permanent	0	1,273	0	2,236	0	2,766	0	530
11.5 - Other personnel compensation	0	4,987	0	4,819	0	4,867	0	48
Overtime	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
Other Compensation	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*
11.8 - Special personal services payments	0	0	0	0	0	0	0	0
Total	**466**	**61,222**	**529**	**75,420**	**550**	**80,067**	**21**	**4,648**
Other Object Classes								
12.1 - Civilian personnel benefits		24,389		29,787		35,623	0	5,835
21.0 - Travel and transportation of persons		402		2,060		2,209	0	149
22.0 - Transportation of things		0		17		0	0	-17
23.1 - Rental payments to GSA		9,356		11,937		12,010	0	73
23.2 - Rental payments to others		318		765		284	0	-481
23.3 - Communications, utilities, and miscellaneous charges		970		672		1,705	0	1,033
24.0 - Printing and reproduction		0		67		36	0	-31
25.1 - Advisory and assistance services		1,998		2,210		2,178	0	-32
25.2 - Other services from non-federal sources		471		1,728		454	0	-1,274
25.3 - Other goods and services from federal sources		5,125		11,040		4,968	0	-6,072
25.4 - Operation and maintenance of facilities		982		1,818		1,293	0	-525
25.7 - Operation and maintenance of equipment		1,097		2,170		1,479	0	-691
26.0 - Supplies and materials		490		1,456		1,485	0	29
31.0 - Equipment		2,960		1,432		3,731	0	2,299
Total Obligations		**109,780**	**529**	**142,579**	**550**	**147,522**	**21**	**4,943**
Net of:								
Unobligated Balance, Start-of-Year		-11,515		-24,424		-20,000	0	4,424
Transfers/Reprogramming		-11,000		-10,400		-10,000	0	400
Recoveries/Refunds		-1,591		-571		-1,666	0	-1,095
Balance Rescission		0		0		0	0	0
Unobligated End-of-Year, Available		24,424		20,000		20,000	0	0
Unobligated End-of-Year, Expiring		467		0		0	0	0
Total Direct Requirements		**110,565**	**529**	**127,184**		**135,856**		**8,672**
Reimbursable FTE								
Full-Time Permanent	68		20		20		0	0
Sub-Allotments and Direct Collections FTE	*5*		*5*		*5*		*0*	

R. Additional Required Information for Congressional Justification

Additional Required Information for Congressional Justification

Office of the Inspector General

The Inspector General Reform Act of 2008 (P.L. 110-409) requires that the Department of Justice OIG submit the following information related

The Aggregate budget request for the operations of the OIG is $145,856,000;

The requested amount includes $525,081 to support the operations of the Council of the Inspector General on Integrity and Efficiency

The portion of the amount needed for OIG training is $1,157,100

The Inspector General of the Department of Justice certifies that the amount requested for training satisfies all OIG training needs of FY23.