



U.S. Department of Justice FY 2025 PERFORMANCE BUDGET

Office of the Inspector General

Congressional Justification



Contents

I.	Overview (Office of the Inspector General).....	1
A.	Introduction	1
B.	Background	1
C.	OIG Organization.....	1
D.	Notable Highlights, Reviews, and Recent Accomplishments.....	3
1.	Strengthening Public Trust in the Department of Justice	3
2.	Strategic Management and Operational Challenges in the Federal Corrections System....	5
3.	Safeguarding and Promoting National Security	9
4.	Enhancing Cybersecurity and Countering Cybercrime	11
5.	Pursuing the Department’s Law Enforcement Mission While Protecting Civil Rights and Civil Liberties.....	12
6.	Improving the Management and Oversight of the U.S. Department of Justice Contracts and Grants.....	14
7.	Effectively Managing Human Capital	17
8.	Whistleblower Program	19
9.	Congressional Testimony.....	20
E.	Challenges	22
II.	Summary of Program Changes.....	23
III.	Appropriations Language and Analysis of Appropriations Language	25
A.	Analysis of Appropriations Language.....	25
IV.	Program Activity Justification.....	26
A.	Audits, Inspections, Investigations, and Reviews	26
B.	Program Description	26
C.	Performance and Resource Tables	27
V.	Performance, Resources, and Strategies.....	30
<hr/>		
A.	Performance Plan and Report for Outcomes.....	30
B.	Strategies to Accomplish Outcomes	30
VI.	Program Increases by Item	31
Item Name: Civil Rights Violations, Cybercrime, and Fraud Investigations		31
Item Name: Cybersecurity and Technology Enhancement		35
Item Name: National Security Programs and Operations Oversight		38

Item Name: Establish OIG’s IT Security & Emerging Technology Oversight Unit.....	43
Item Name: Cybersecurity and Information Technology Division Enhancement.....	48
Item Name: Prison Inspections Program Enhancement.....	53
VII. Appendix	58
A. Statistical Highlights	58
<hr/>	
VIII. Exhibits	59
A. Organizational Chart	59
B. 1. Summary of Requirements.....	60
B. 2. Summary of Requirements by Decision Unit	61
C. Summary of Requirements by Decision Unit	62
D. Resources by DOJ Strategic Goal and Objective.....	63
E. Justification for Technical and Base Adjustments	64
F. Crosswalk of 2023 Availability.....	65
G. Crosswalk of FY 2024 Availability	66
H.R. Summary of Reimbursable Resources	67
H.S. Summary of Sub-Allotments and Direct Collections Resources.....	68
I. Detail of Permanent Positions by Category	69
J. Financial Analysis of Program Changes	70
K. Summary of Requirements by Object Class	71
R. Additional Required Information for Congressional Justification.....	72

I. Overview (Office of the Inspector General)

A. Introduction

In Fiscal Year (FY) 2025, the President's budget request for the Department of Justice (the Department or DOJ) Office of the Inspector General (OIG) totals \$171.590 million, which includes \$10 million for Crime Victims Fund (CVF) oversight (\$5 million as a technical base adjustment and \$5 million as a direct transfer), 578 direct positions (150 agents and 50 attorneys) plus 22 reimbursable positions to investigate allegations of fraud, waste abuse, and misconduct by DOJ employees, contractors, and grantees and to promote economy and efficiency in Department operations. After mandatory base adjustments are considered, this request is an 8.5% increase from the FY 2024 Annualized Continuing Resolution. Additionally, the OIG is requesting \$4.0 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 investigates alleged violations of fraud, abuse, and misconduct by DOJ employees, contractors, grantees, and other outside parties. The Division's Special Agents develop cases for criminal or civil prosecution, or administrative action. The Investigations Division has seven regions with offices in Arlington, Atlanta, Boston, Chicago, Dallas, Denver, Detroit, El Paso, Houston, Los Angeles, Miami, New York, San Francisco, Trenton, and Tucson. Its Fraud Detection Office and Cyber Investigations Office are co-located in Arlington, VA, with personnel in offices nationwide. Investigations Headquarters in Washington, D.C. consists of the Immediate Office of the Assistant Inspector General for Investigations and the following branches: Operations I, Operations II, Investigative Support, Administrative Support, and Hotline Operations.

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 information technology 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

At its core, public service is a public trust. The DOJ earns public trust through transparency and its impartial administration of justice. Eroded public trust represents a significant and concerning challenge that weakens the Department's ability to fulfill its mission to uphold the rule of law, to keep our country safe, and to protect civil rights. Ensuring that decision making adheres to established Department policies and practices, is free from inappropriate influences, and complies with conflicts of interest rules are key elements to meeting this challenge. In addition, DOJ should be attentive to addressing perceived disparities in law enforcement responses to significant events, consistency and objectivity in the use of sensitive law enforcement authorities and demonstrating honesty and integrity in the performance of duties.

Examples of OIG Work:

An Investigation of Alleged Misconduct by United States Attorney Rachael Rollins

In May 2023, the OIG issued a report describing an investigation of alleged misconduct by U.S. Attorney for the District of Massachusetts Rachael Rollins. The evidence the OIG obtained substantiated multiple allegations concerning Rollins. Most concerning, the OIG found that Rollins used her position as U.S. Attorney and used non-public DOJ information available to her by virtue of her position as U.S. Attorney, in an effort to influence the outcome of an election, in violation of the Standards of Ethical Conduct for Employees of the Executive Branch, as well as Department policy and the obligations under the Ethics Agreement she signed after her nomination as U.S. Attorney. The OIG also found that Rollins actively participated in a partisan political campaign, in violation of Department policy that further restricts the political activity of noncareer officials, including U.S. Attorneys and that she knowingly and willfully made a false statement of material fact and lacked candor during her OIG interview. The OIG also found that, among other things, Rollins attended a partisan political fundraiser without approval from the Deputy Attorney General, or her designee, as required by Department policy, and her attendance was contrary to the ethics advice she received before the event.

Former FBI Special Agent Sentenced for Conspiracy to Commit Bribery of a Public Official, Bribery of a Public Official, and Money Laundering

In February 2023, a former FBI Special Agent (SA) was sentenced to 72 months of imprisonment, 3 years of supervised release, and ordered to forfeit \$132,309 and pay a \$30,000 fine for conspiracy to bribe a public official, bribery of a public official, and money laundering. According to evidence presented at trial, the SA accepted cash bribes, private jet flights, a motorcycle, hotel stays, escorts, meals, and other items from an organized crime-linked lawyer. In return, the SA conducted law enforcement database inquiries and used those inquiries to help the lawyer and his associates avoid prosecution and law enforcement monitoring.

Finding of Misconduct by an FBI Management and Program Analyst for Unauthorized Communications with Members of the Media, for Disclosing Sensitive Information to a Reporter, for Lack of Candor, and for Accepting Prohibited Gifts

In January 2023, the OIG completed its report of investigation for an investigation initiated upon the receipt of information from the FBI concerning possible unauthorized communications by a Management and Program Analyst (MAPA) with a member of the media. The MAPA resigned from the FBI in September 2019, after the FBI suspended the MAPA's security clearance. The

investigation was presented for prosecution on May 21, 2019, and declined on July 8, 2019. The OIG completed its investigation and provided its report to the FBI.

Audit of the Roles and Responsibilities of the FBI's Office of the General Counsel in National Security Matters

At the request of former Attorney General Barr, the OIG conducted an audit of the FBI's Office of the General Counsel's roles and responsibilities in national security matters. The OIG's September 2022 audit report revealed a relationship between the FBI's Office of the General Counsel and the National Security Division that historically has been strained and hindered by overlapping or undefined responsibilities and miscommunication in national security matters, thereby affecting coordination needed to ensure the effectiveness of the FBI's national security program. The DOJ as a whole has an essential responsibility to carry out its critical investigative and national security duties in an effective manner and to do so with efficient coordination while maintaining focus on adhering to the rule of law and upholding the public's confidence. The OIG found that these coordination efforts need to be improved, and roles and responsibilities should be more clearly defined. The report contains five recommendations to the FBI and DOJ to improve oversight of the FBI's national security activities.

Management Advisory Memorandum: Recommendations Regarding the Immigration Judge and Board of Immigration Appeals Member Hiring Process

Alleged politicized hiring of Immigration Judges within the Executive Office of Immigration Review led members of Congress to ask the OIG to investigate whether Immigration Judge and Board of Immigration Appeals positions were withdrawn, delayed, or favored for political or ideological reasons. The OIG did not find evidence of systemic politicized hiring. However, in March 2022, we issued a MAM recommending that the Executive Office for Immigration Review update its hiring process to clarify that candidates are evaluated and selected without regard to perceived political affiliation or ideology. Such steps will help to ensure transparency and accountability in these processes.

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.

Between January 1, 2023, and June 30, 2023, the period covered by this report, the OIG processed 1,562 new complaints that were identified by the complainant as civil rights or civil liberties complaints. Of these complaints, 1,536 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 26 of the 1,562 complaints it received involved DOJ employees or DOJ components and included allegations that required further review. The OIG determined that 25 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. One of the 26 complaints was referred to the OIG's Oversight and Review Division for review because it raised employment retaliation allegations unrelated to Section 1001 of the PATRIOT Act.

Ongoing Work:

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 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.

Investigation Into Use of Force Allegations Involving DOJ Law Enforcement Personnel in Portland, Oregon

In response to Congressional requests, complaints received by the OIG, and a referral from the U.S. Attorney in Oregon, the OIG has opened an investigation into use of force allegations involving DOJ law enforcement personnel in Portland, Oregon in July 2020. The DOJ OIG will coordinate our investigation with the Department of Homeland Security OIG.

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.

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

The federal prison system, which is managed by the Department's Federal Bureau of Prisons (BOP), is a critical part of its criminal justice mission. The BOP continues to be the largest DOJ employer. For at least the past decade, the OIG reports have found weaknesses and failures in the management of BOP operations and have made dozens of recommendations to address them. We also have consistently identified managing the federal prison system as one of the most significant and important management challenges facing the Department. Among the significant recurring issues the OIG has identified in our oversight of the BOP are staffing and internal audits; deaths in custody; professionalism and accountability of staff; institutional safety and security, including deteriorating facilities; cost and quality of inmate healthcare, including mental health; and policy development. Adequately addressing these issues is integral to the

BOP's and the Department success in ensuring a safe, humane, and compassionate federal prison system.

Examples of OIG Work:

Notification of Concerns Regarding the Federal Bureau of Prisons' Use of Temporary Secure Enclosures with Limited Space for Lengthy Time Periods

In December 2023, the OIG issued a Management Advisory Memorandum advising the BOP of concerns arising from BOP's use of secure enclosures with limited space to hold inmates for lengthy periods at its facilities. The OIG identified these concerns during an investigation in which an inmate, during an Immediate Use of Force, was placed in such a secure enclosure measuring three feet wide by three feet deep and seven feet tall for approximately 21 hours. During this investigation and other investigations, we learned that it is a common practice for BOP employees to utilize secure enclosures of these or similar dimensions to temporarily hold inmates for various reasons, such as when there is a need to leave the inmate temporarily unattended while moving the inmate between standard cells or to other locations within a facility. However, the BOP does not have any written guidance regarding the use of temporary secure enclosures, such as the appropriate size, the length of time an inmate may remain in such an enclosure, or how an inmate should be monitored while in the secure enclosure. In this memorandum, the OIG made two recommendations to address the concerns identified.

Inspection of the Federal Bureau of Prisons' Federal Correctional Institution Tallahassee

In November 2023, the OIG issued a report with findings regarding the unannounced Inspection of the FCI Tallahassee Institution. The inspection identified several serious operational deficiencies. Among the most concerning were the alarming conditions of its food service and storage operations. Specifically, on our second day at the institution, we observed inmates being served moldy bread and vegetables rotting in a refrigerator in a food preparation area at the female prison. We also observed in food storage warehouses likely evidence of rodent droppings and rodents having chewed through boxes of food, as well as bags of cereal with insects in them and warped food containers. The OIG also identified in the female prison serious infrastructure problems that created unsanitary and potentially unsafe conditions. The OIG also found that FCI Tallahassee's Health Services Department is experiencing significant staffing shortages, with 38 percent of its positions vacant, which is consistent with challenges associated with hiring healthcare professionals across the BOP.

Audit of the Federal Bureau of Prisons' Contract Awarded to the American Correctional Association (ACA)

In November 2023, the OIG issued a report of an audit which evaluated: (1) the value the BOP receives through ACA accreditation for its prisons; (2) how the BOP uses ACA's accreditation to improve BOP standards for health, safety, and security of inmates and staff; and (3) the BOP's contract administration and ACA's performance and compliance with terms, conditions, laws, and regulations applicable to the contract. As a result of the audit, the OIG found that ACA's reaccreditation reviews were reliant on the BOP program review process. We found that the BOP and ACA modified ACA's reaccreditation process, eliminating an intensive review of BOP facility documentation, which is not specifically noted in the contract's Statement of Work, and relied on the BOP program reviews. The OIG has numerous concerns about the lack of independence in this process, which is inconsistent with the BOP's stated intent for this contract – that is, to have an independent assessment of each institution's operations and programs. This OIG is also concerned that external stakeholders and the general public are not aware that ACA

did not perform its standard reaccreditation process for BOP facilities, which creates a potential misconception that all correctional facilities are reviewed for ACA accreditation in the same manner. Based on these concerns, we do not believe that ACA's reaccreditation of BOP facilities valuably enhances the BOP's operations and programs. The audit also identified issues with the BOP's administration and oversight of its contract with ACA. Additionally, the BOP did not have a consistent process in place to ensure ACA's billings were accurate, complete, and paid timely. The OIG made 10 recommendations to the BOP.

Investigation and Review of the Federal Bureau of Prisons' Custody, Care, and Supervision of Jeffrey Epstein at the Metropolitan Correctional Center in New York, New York

In June 2023, the OIG issued a report with findings regarding MCC New York personnel's custody, care, and supervision of Epstein while detained at the facility from his arrest on federal sex trafficking charges on July 6, 2019, until his death on August 10, 2019. The OIG made eight recommendations to the BOP to address the numerous issues identified during our investigation and review. Finally, the OIG recommended that the BOP review the conduct and performance of the BOP personnel as described in this report and determine whether discipline or other administrative action with regard to each of them is appropriate.

Audit of the Federal Bureau of Prisons' Efforts to Construct and Maintain Institutions

In May 2023, the OIG issued an audit report of the BOP's efforts to construct and maintain institutions. The OIG found that the BOP's ability to address its infrastructure requirements is limited by the absence of a well-defined infrastructure strategy and the limited amount of funding it has requested through the budgeting process, and therefore received from Congress. This resource challenge affects the BOP's ability to modernize its facilities and results in increasingly costly maintenance and repairs and, in the most extreme circumstances, shuttering institutions and relocating inmates when the inability to complete the needed maintenance and repairs results in unsafe conditions.

Inspection of the BOP's FCI Waseca

In May 2023, the OIG issued a report and found that FCI Waseca suffers from a shortage of COs and its Health Services and Psychology Services Departments have significant staffing shortages, causing delays in treatment of the physical and mental healthcare needs of inmates.

Additionally, the OIG identified serious infrastructure issues, including significant damage to several building roofs that have caused leaks throughout the institution, damaged medical and dental equipment, and rendered certain rooms and cells unusable. In addition, the OIG found that FCI Waseca's existing security camera system produces low resolution video, making it difficult to monitor inmate activity, and there are not enough cameras to provide sufficient coverage of the institution. The OIG did not make any recommendations for this report.

However, related to past reports and recommendations, the OIG will continue to monitor the BOP's efforts to address these systemic issues at all BOP institutions, including FCI Waseca.

Limited-Scope Review of the Federal Bureau of Prisons' Strategies to Identify, Communicate, and Mitigate Operational Issues at Its Institutions

In May 2023, the OIG issued a limited-scope review report of the strategies the BOP employs to identify, communicate, and mitigate operational issues at its institutions. The OIG initiated this limited-scope review after certain operational issues became so serious at U.S. Penitentiary (USP) Atlanta and Metropolitan Correctional Center (MCC) New York that, in 2021, the BOP significantly limited operations at the former and closed the latter. BOP Executive Staff members in place in 2021 and 2022 told us that they had been largely aware of long-standing

operational issues at USP Atlanta and MCC New York. Nevertheless, the OIG found that the BOP's then-Executive Staff was not able to take actions to effectively remedy them. The OIG made five recommendations to help the BOP ensure that its institutions operate safely and effectively. The BOP concurred with all five recommendations.

Evaluation of the Federal Bureau of Prisons' Efforts to Address Sexual Harassment and Sexual Assault Committed by Inmates Toward Staff

In February 2023, the OIG evaluation found that inmate-on-staff sexual harassment is widespread within the BOP and that BOP staff believe that it particularly affects female employees. The BOP does not collect adequate data on inmate-on-staff sexual harassment and has been unable to identify the prevalence and scope of the issue, which prevents the BOP from evaluating the effectiveness of its mitigation strategies. Also, training on inmate-on-staff sexual harassment needs further updating. The OIG made nine recommendations to the BOP; these relate to assessing the full scope of inmate-on-staff sexual harassment across the BOP and increasing the effectiveness of the BOP's mitigation efforts.

Ongoing Work:

Review of Federal Bureau of Prisons Inmate Deaths in Custody

The OIG is conducting a review of non-natural inmate deaths at BOP institutions, from fiscal years 2014 through 2021. This review will assess the circumstances surrounding inmate deaths and evaluate how the BOP seeks to prevent future inmate deaths.

Department of Justice Office of the Inspector General Announces Initiation of Investigation of the circumstances surrounding the release from prison and subsequent death of Frederick Marvin Bardell,

The OIG is investigating the circumstances surrounding the release from prison and subsequent death of Frederick Marvin Bardell, who was released from the Seagoville Federal Correctional Institution in Seagoville, Texas, on February 8, 2021, and died 9 days later. In an order dated October 4, 2022, Judge Roy B. Dalton, Jr., in the U.S. District Court, Middle District of Florida, who had previously reviewed Mr. Bardell's petitions for compassionate release, recommended that the Attorney General, the OIG, or other appropriate investigative offices undertake an examination into the conditions of Mr. Bardell's confinement and treatment, and alleged misrepresentations to the Court. The OIG initiated this investigation in response to the allegations in Judge Dalton's order and will conduct its investigation consistent with the OIG's jurisdiction as established in the Inspector General Act of 1978, as amended. If circumstances warrant, the OIG will consider including other issues that may arise during the course of the investigation.

Audit of the Federal Bureau of Prisons' Inmate Financial Responsibility Program

The OIG is conducting an audit of the BOP's Inmate Financial Responsibility Program (IFRP). The IFRP helps federal offenders develop a financial plan for meeting court-ordered and other legitimate financial obligations while incarcerated in BOP institutions, including, in many cases, payments to victims. The preliminary objectives are to: (1) examine the BOP's administration of the IFRP, and (2) assess the IFRP's controls over inmate payments to satisfy court-ordered obligations.

Audit of the Federal Bureau of Prisons' Management of its National Gang Unit

The OIG is conducting an audit of the BOP's management of its National Gang Unit. Our preliminary objectives are to: (1) evaluate the BOP's management of the National Gang Unit; and (2) evaluate the National Gang Unit's process for identifying, designating, and tracking incarcerated gang members.

3. Safeguarding and Promoting 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.

Examples of OIG Work:

Audit of the Department of Justice's Strategy to Address the Domestic Violent Extremism Threat

In June 2023, the OIG issued a report of the Department's strategy to address Domestic Violent Extremism (DVE). The Department has undertaken efforts to implement the first-ever National Strategy for Countering Domestic Terrorism, released by the White House in June 2021, but does not have a formal Department-wide strategy or framework to guide its efforts. The OIG found that the DOJ has experienced challenges in ensuring that its various DVE-related enforcement, grantmaking, and outreach efforts are cohesive and used in a strategic way to better identify lessons learned and spread awareness of available resources. In March 2021, the Department issued guidance to federal prosecutors regarding the identification and coordination of investigations and prosecutions with a nexus to DVE, and this guidance was codified and clarified in revisions to Section 9-2.137 of the Justice Manual in November 2022. During the audit period, however, the OIG found that the DOJ's litigation and law enforcement components may not all have had the same understanding of what constitutes a DVE nexus and may not all have been aware of the need to identify and report DVE-related cases consistently. Given the significant risks associated with combating DVE-related threats while also protecting civil liberties and maintaining public confidence in the Department's objectivity in addressing this threat, the DOJ should continue to enhance its mechanisms to routinely evaluate the efficacy and impact of its DVE efforts. Further, the DOJ should evaluate and deconflict its efforts to track DVE-related cases to ensure it has an accurate understanding and prioritization of the threat, which will help to promote transparency with stakeholders.

Audit of the Federal Bureau of Investigation's National Security Undercover Operations

In December 2022, the OIG issued an audit report examining the FBI's management of its national security Undercover Operations (UCOs). A UCO is a series of related undercover activities by Undercover Employees (UCEs) or Online Covert Employees (OCEs) who, under alias, engage directly or indirectly in relationships or communications with predicated targets over an extended period, while concealing their FBI affiliation. The use of undercover techniques can be an effective and important investigative tool for counterterrorism, counterintelligence, and the investigation of cyber-based crimes. However, without robust management and oversight, UCOs may increase the risk to the safety and wellbeing of FBI personnel or to the operational security of ongoing investigations. The OIG found several areas for improvement in the FBI's management and oversight of its UCOs. The OIG made

10 recommendations to improve the operational security and management of the FBI's undercover operations. The FBI agreed with all 10 recommendations.

Audit of the Roles and Responsibilities of the FBI's Office of the General Counsel in National Security Matters

In September 2022, the OIG issued an audit report that found the relationship between the FBI's Office of General Counsel and the National Security Division (NSD) is historically strained and at times hindered by overlapping or undefined responsibilities and miscommunication. The OIG's findings include: (1) clarity needed regarding the roles of the attorneys within the FBI Office of General Counsel's National Security and Cyber Law Branch (NSCLB) and NSD in providing legal advice and guidance, (2) FBI's recordkeeping of its notices to the Foreign Intelligence Surveillance Court needs improvement, (3) joint National Security Reviews by NSD and NSCLB were untimely and lacked consensus, (4) differing legal views by NSCLB and NSD, and (5) the Foreign Intelligence Surveillance Act of 1978 use request process needs improvement. The OIG made five recommendations to the FBI and the Office of the Deputy Attorney General. The FBI and the Office of the Deputy Attorney General agreed with all five recommendations.

Audit of the Office of Justice Programs National Institute of Justice Using Artificial Intelligence Technologies to Expose Darknet Opioid Traffickers Grant Awarded to the West Virginia University Research Corporation, Morgantown, West Virginia

An OIG audit report issued in September 2022 found that five publications, which were partly researched and developed under a grant NIJ awarded to develop a prototype law enforcement system that detects opioid trafficking participants on the dark web, listed co-authors with affiliations to foreign research institutions on the U.S. government's Entity List. The U.S. Entity List identifies entities or individuals that the U.S. government has determined have been involved, are involved, or pose a significant risk of being or becoming involved in activities contrary to the national security or foreign policy interests of the United States. Although the OIG did not find evidence of any wrongdoing, potential inappropriate knowledge transfers, or undue foreign influence stemming from these co-authorships, underscores the significant risks DOJ must protect against to ensure that the knowledge gained, or technology developed from taxpayer-funded Departmental research is not at risk of being exported to support foreign governments or non-state actors with interests adversarial to the United States.

Ongoing Work:

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

The OIG is reviewing DOJ's efforts to coordinate the sharing of information related to malign foreign influence on U.S. elections. The objectives of this review are to (1) assess the effectiveness and resilience of the Department's information sharing system related to malign foreign influence on elections; (2) assess the Department's oversight, management, and coordination of its activities to respond to malign foreign influence on elections; and (3) identify any gaps in or duplication of its information sharing efforts.

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.

4. Enhancing Cybersecurity and Countering Cybercrime

The Department faces the challenge of leveraging law enforcement, legal, information technology, and intelligence resources, along with public-private partnerships and international partnerships, when managing cyber-related threats and emerging technologies. Like technology itself, these areas are continuously evolving. Additionally, the number and scale of major cyber incidents—some of which can involve tens of thousands of victims—are growing and challenging DOJ's ability to respond.

Examples of OIG Work:

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

In July 2022, the OIG issued an audit report examining DOJ's cyber supply chain risk management (C-SCRM) efforts. The objective was to determine the extent to which the Department, through the Justice Management Division (JMD) and the FBI, implemented an organizational C-SCRM program that identifies, assesses, mitigates, and responds to supply chain risk throughout the information technology lifecycle.

The OIG found that overall, JMD lacked the personnel resources to effectively manage its C-SCRM program, resulting in widespread noncompliance, outdated C-SCRM guidance, inadequate threat assessments, and insufficient mitigation and monitoring actions. These weaknesses increase the risk of introducing products or services into DOJ's IT environment that could compromise the integrity of its systems and data. While the FBI's program is more modern than JMD's, it too has several processes and deliverables in need of enhancement. FBI procurement officials often improperly bypassed its C-SCRM program entirely, due in part to a misunderstanding or unawareness of the C-SCRM requirements.

As of August 31, 2023, 15 of the 17 recommendations made by the OIG to assist the Department in managing cyber supply chain risks remained open. Addressing the open recommendations will help JMD and the FBI enhance risk mitigation and monitoring of the risk across all DOJ components.

Audit of the United States Marshals Service's Management of Seized Cryptocurrency

In June 2022, the OIG issued an audit report that assessed the USMS's handling of about \$466 million in seized cryptocurrency from FYs 2017-2021. The audit found that although the USMS implemented adequate safeguards for the storage of and access to seized cryptocurrency, the USMS faces challenges with managing and tracking its seized cryptocurrency in DOJ's Consolidated Asset Tracking System. The audit also found that USMS policies related to storage, quantification, valuation, and disposal are inadequate, absent, and in some instances provide conflicting guidance. The OIG made seven recommendations to improve the USMS's management and tracking of seized cryptocurrency.

Federal Information Security Modernization Act Audits

The Federal Information Security Modernization Act (FISMA) requires the Inspector General for each agency to perform an annual independent evaluation of the agency's information security programs and practices. Each evaluation includes (1) testing the effectiveness of information security policies, procedures, and practices of a representative subset of agency systems; (2) an assessment (based on the results of the testing) of compliance with FISMA; and (3) separate representations, as appropriate, regarding information security related to national security systems. The Office of Management and Budget (OMB) is responsible for the submission of the annual FISMA report to Congress. The Department of Homeland Security prepares the FISMA metrics and provides reporting instructions to agency Chief Information Officers, Inspectors General, and Senior Agency Officials for Privacy. The evaluation includes testing the effectiveness of information security policies, procedures, and practices of a representative subset of agency systems. The FY 2023 FISMA results were submitted to the OMB in September 2023.

As of September 2023, there are currently 47 open FISMA recommendations from all FISMA audits conducted across the Department, indicating that work remains to be done.

Ongoing Work:

Audit of the Federal Bureau of Investigation's Efforts to Respond to Changing Operational Technologies

The OIG initiated an audit of the FBI's efforts to respond and adapt to changing technologies in the environments where it operates. Our preliminary objectives are to determine 1) the sufficiency and effectiveness of the actions that the FBI is taking to respond to changing technological environments and 2) the training the FBI provides to its personnel to increase the work force's adaptability to those changes.

Audit of the Department of Justice's Strategy to Combat and Respond to Ransomware Threats and Attacks

The OIG initiated an audit of the Department's strategy to combat and respond to ransomware threats and attacks to assist DOJ in meeting this enormous challenge. This audit's objectives are to assess the Department's (1) strategy to combat ransomware threats, and (2) response to and coordination on ransomware attacks against public and private entities.

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

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

Examples of OIG Work:

Audit of the Department of Justice's Law Enforcement and Corrections Components' Use-of-Force Policies

In September 2023, the OIG issued an audit report identifying whether the Department law enforcement and corrections components updated their policies align with DOJ's updated use-of-force guidance and requirements. The OIG identified certain policy gaps related to use-of-force in custodial situations. In addition, some components' policies and practices for the use-of-force were inconsistent in their application to task force officers and contractors. The Department also has not identified a mechanism to help ensure components' training programs are consistent, appropriate, or complete. The OIG made six recommendations to minimize potential risks associated with use-of-force tactics, including addressing policy gaps at the Department and component levels.

Audit of the Office of Justice Programs' Civil Rights Complaint Process

In September 2023, the OIG issued a report assessing how the Office of Justice Programs' (OJP) Office for Civil Rights (OCR) solicited, received, and reviewed complaints of unlawful discrimination by recipients of DOJ grants and cooperative agreements from FY 2019 through FY 2022. Overall, the review found that certain aspects of OJP OCR's civil rights complaint process could be improved. The report contains six recommendations to improve OJP's administration and oversight of the civil rights complaint process, and OJP agreed.

Audit of the Bureau of Alcohol, Tobacco, Firearms and Explosives' Risk-Based Inspection Selection Processes and Administrative Actions Issued to Federal Firearms Licensees

In April 2023, the OIG released a report assessing ATF's: (1) risk-based approach for managing federal firearms licensee (FFL) inspections, (2) certain activity related to the referral of FFL-related information for criminal investigation, and (3) processing of FFL revocations and other administrative actions. In prior reports, the OIG identified resource challenges facing ATF and issued recommendations to ATF to improve its oversight of FFLs. Although ATF has taken action to address those recommendations, this audit again identified concerns with ATF's oversight of FFLs. The OIG identified 13 recommendations for ATF to strengthen its compliance inspection activities and its oversight of FFLs. Specifically, the OIG recommended that ATF develop modern tools, such as employing predictive analytics, and that ATF revise its policies and procedures concerning the examination of inspection results to effectively identify high-risk FFLs. Implementing these recommendations could help enable ATF to not only increase the number of FFL inspections as described in DOJ's strategic plan, but also increase the efficacy of those inspections.

Ongoing Work:

Audit of the Federal Bureau of Investigation's Handling of Tips of Hands-on Sex Offenses Against Children

The OIG is conducting an audit of the FBI's handling of tips of hands-on sex offenses against children. The preliminary objective is to evaluate the FBI's compliance with laws, regulations, and policies related to its handling of tips of hands-on sex offenses against children and mandatory reporting of suspected child abuse.

Audit of the Implementation of the DOJ Electronic Recording of Statements Policy

The OIG is conducting an audit on the Department of Justice's Policy 9-13.001, which governs the electronic recording of custody statements of four components: the Bureau of Alcohol, Tobacco, Firearms and Explosives; Drug Enforcement Administration; Federal Bureau of Investigation; and U.S. Marshals Service. The preliminary objective is to assess component-level policies and procedures implemented to effectuate the DOJ Electronic Recording of Statements Policy.

Audit of the U.S. Marshals Service's Special Deputation Authority

The OIG is conducting an audit of the USMS's special deputation authority. The preliminary objective is to assess whether the USMS has established adequate policies, procedures, and controls to manage the Special Deputation Program.

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

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.

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

In FY 2023, the Department awarded over \$9.61 billion in contracts and over \$5.66 billion in grants. Effective management of contract and grant awards to ensure financial accountability and mitigate the risks of fraud or misuse is an ongoing challenge for the Department. Some of those challenges include complying with laws, regulations, and policies that govern contract workers' rights and protections, acquisition planning, and contract oversight and administration. Additionally, monitoring grants and ensuring the functionality of the Department's grants management system have remained pressing challenges for the DOJ.

Examples of OIG Work:

Audit of the Community Relations Service's Contracting Activities

In August 2023, the OIG issued a report identifying instances where Community Relations Service (CRS) did not comply with FAR and DOJ requirements during the acquisition and procurement phases, including requirements pertaining to acquisition planning, market research, and whistleblower notification. Additionally, we found deficiencies related to CRS's administration and oversight of contracts, such as CORs not being certified and not always being properly designated, inadequate review of billed labor charges, and untimely payments. OIG also identified several instances where CRS directed a contractor to make purchases under support services contracts and the purchases were not specifically tied to a contract deliverable or work requirement. These weaknesses in how CRS performed its contracting activities created an environment that increased the risk of failing to safeguard the federal government's financial interests.

Audit of the Office of Justice Programs' Procurement for the JustGrants System

In July 2023, the OIG issued a report that found the OJP's planning and development process was insufficient to meet the non-negotiable "go live" deadline, and the OJP faced challenges in implementing JustGrants. When the system went live in October 2020 with only about 30 percent of planned system features completed, users were faced with significant technical issues that adversely affected their ability to administer awards and conduct necessary oversight. Further, the OIG identified issues with the OJP's administration, oversight, and monitoring of the BPA which, if improved, will assist the OJP in additional IT modernization efforts under this award and with future procurements.

Audit of the Bureau of Alcohol, Tobacco, Firearms and Explosives' Enterprise Standard Architecture Task Order V Awarded to Leidos, Inc.

The OIG identified significant issues with ATF's \$492.7 million contract with Leidos for information technology services that led to cost increases and the government's inability to hold Leidos accountable for poor performance. Federal components expressed dissatisfaction with Leidos' work performance and delays in getting work accomplished due to Leidos contesting that assigned work was out of scope. These delays left risks to government IT systems insufficiently mitigated within required timeframes. The OIG found that the contract's shared cost model and the cost variability may negatively impact agency budgets. Despite federal components descopeing services or leaving the program, the overall contract value had increased 85 percent. The OIG made eight recommendations, and ATF concurred with five recommendations and partially concurred with three recommendations. Leidos partially agreed with one recommendation and stated that it was not in a position to agree or disagree with the remaining recommendations.

Audit of the Office of Justice Programs Cooperative Agreement Awarded to Community Resources for Justice, Incorporated, Boston, Massachusetts

The OIG released a report on one cooperative agreement totaling \$8,446,180 awarded to Community Resources for Justice (CRJ) for the purpose of supporting a multistage process in which a state increases the cost effectiveness of its criminal justice system and reinvest savings into high performing public safety strategies. The OIG found that CRJ could improve certain areas of its grant administration, including fringe benefit, travel expenditures, and subrecipient monitoring. The OIG identified \$30,292 in unsupported questioned costs. The OIG made five recommendations to OJP to improve CRJ's management of award performance, and OJP agreed with all of them. CRJ agreed with two recommendations and neither agreed nor disagreed with the remaining three recommendations.

Examples of the OIG CVF Grant Work:

Audit of the Office of Justice Programs Victim Assistance Funds Subawarded by the Georgia Criminal Justice Coordinating Council to Women Moving On (WMO), Inc., Decatur, Georgia

In June 2023, the OIG issued a report with four recommendations for OJP and the Georgia CJCC to assist WMO in improving its award management and administration and to remedy unallowable and unsupported costs. The OJP provided funds to the Georgia Criminal Justice Coordinating Council (Georgia CJCC) to make subawards supporting victim assistance programs in the state of Georgia. The Georgia CJCC awarded \$1,703,090 in crime victim assistance funds to Women Moving On, Inc. (WMO), under two subawards in October 2020 and one subaward in October 2021. The purpose of the subawards was to provide services to victims of domestic violence. As of November 2022, the Georgia CJCC had reimbursed WMO the total of the three

subawards, \$1,703,090. The audit concluded that WMO needs to establish comprehensive written policies and procedures to ensure its financial records accurately reflect all expenditures charged to VOCA subawards and that payments made by WMO are made according to the VOCA Victim Assistance Program requirements. WMO lacked segregation of duties, circumvented internal controls procedures over disbursement of funds, and did not disclose to the Georgia CJCC a potential conflict of interest.

Audit of the Office of Justice Programs Victim Compensation Grants Awarded to the Arkansas Department of Public Safety, Little Rock, Arkansas

In May 2023, the OIG issued a report for an audit assessing Arkansas Department of Public Safety's (DPS) overall process for making victim compensation payments. The OIG also assessed Arkansas DPS's policies and procedures for providing compensation payments to victims, as well as the accuracy of the state certification forms. The Office for Victims of Crime (OVC) awarded these grants, totaling \$2,746,000 from FY 2019 to 2021, from the Crime Victims Fund to provide financial support through the payment of compensation benefits to crime victims throughout Arkansas. As of December 2022, Arkansas DPS drew down a cumulative amount of \$2,391,261 for the grants we reviewed. Overall, the OIG found that Arkansas DPS established a program to compensate victims and survivors of criminal violence and made efforts to bring awareness to the program. However, the OIG found that Arkansas DPS had a practice that required victims to provide a social security or visa number to receive direct victim compensation payments. Also, the OIG identified issues with the accuracy of Arkansas DPS's state certification forms and performance reports.

Audit of the Office of Justice Programs Victim Assistance Grants Awarded to the New York Office of Victim Services (OVS), Albany, New York

In May 2023, the OIG released a report on two grants totaling \$331,383,703 awarded to the NY OVS, which coordinates with criminal justice agencies in New York on victim and witness service initiatives and priorities and serves as a liaison for the agency with various crime victim coalitions, federal authorities, the public, and other interested parties. The OIG determined that NY OVS should improve subgrant data reporting, written policies and procedures, subrecipient monitoring, and utilization of its VOCA funds to reduce the amount of unspent funding. The OIG made four recommendations to the OJP and NY OVS, and OJP agreed with all of them. NY OVS agreed with three of them and disagreed with one recommendation, for which it provided corrective actions and requested closure of the recommendation.

Audit of the Office of Justice Programs Victim Compensation Grants Awarded to the Alabama Crime Victims Compensation Commission (CVCC), Montgomery, Alabama

In May 2023, the OIG released a report on three OJP grants totaling over \$4.5 million awarded to the Alabama CVCC. The OIG found that though the Alabama CVCC compensated victims and survivors of criminal violence, it needs to improve controls over reporting. Specifically, the Alabama CVCC did not implement adequate procedures to compile and submit accurate annual performance reports and state certification forms, increasing the risk that the Alabama CVCC provided an incomplete description of the value and benefits of its program. The OIG made three recommendations to OJP to improve Alabama CVCC's management of grant performance, and OJP agreed and the Alabama CVCC concurred with all of them.

Audit of the Office of Justice Programs Victim Compensation Grants Awarded to the Office of Kansas Attorney General, Topeka, Kansas

In June 2023, the OIG released a report on three grants totaling \$4,296,000 awarded to the Kansas AG. The OIG identified issues related to Kansas AG's accounting policies and procedures, financial reporting, and drawdowns. Specifically, the OIG found that Kansas AG did not track expenditures for awards separately in its accounting system. Additionally, the OIG identified \$40,772 in unallowable questioned costs. The OIG made five recommendations to the OJP, and the OJP agreed and Kansas AG concurred with all of them.

7. Effectively Managing Human Capital

The DOJ faces an array of human capital challenges, including fostering a workplace that is free from sexual misconduct, sexual harassment, and inappropriate relationships; ensuring equity in hiring and advancement of employees; and identifying and engaging in successful recruitment and retention policies and practices, particularly post-pandemic, to ensure that the Department remains competitive in the market for the most capable and diverse talent.

Examples of OIG Work:

Management Advisory Memorandum – Notification of Concerns Identified in the Drug Enforcement Administration's Use of Polygraph Examinations in Pre-employment Vetting

In August 2023, the OIG issued a report identifying significant risks involving the DEA's polygraph program, including hiring SAs and Intelligence Research Specialists who have not successfully completed some or all of the polygraph examination and allowing task force officers who have failed the polygraph examination to remain on DEA Task Forces. The OIG found inconsistencies in the implementation of the DEA's 2019 polygraph policy. Specifically, the OIG found that the DEA hired 77 applicants who did not pass the pre-employment polygraph examination because the DEA continued to use job announcements that were issued prior to the 2019 policy. Additionally, the OIG determined the DEA hired and entered on duty at least three SAs who did not meet DEA requirements to fully complete a pre-employment polygraph examination, namely both the Suitability and National Security polygraph. The OIG made five recommendations, and the DEA concurred with all of them.

Investigative Summary: Findings of Misconduct by a DOJ Information Technology Specialist for Disparaging and Racist Remarks and a Threatening Statement, Failure to Properly Escort Visitors and to Follow Mail Screening Policy, and Lack of Candor

In February 2023, the OIG issued an investigation report that found the DOJ IT Specialist made disparaging and racist remarks about a colleague as well as made a threatening statement in the workplace, in violation of DOJ policy and federal regulations. The OIG investigation further found the DOJ IT Specialist failed to properly escort visitors at a federal facility, in violation of DOJ policy, and failed to follow mail screening policy. Finally, the OIG investigation found that the DOJ IT Specialist lacked candor during an interview with the OIG, in violation of DOJ policy.

Investigative Summary: Findings of Misconduct by an Assistant United States Attorney for Sexually Inappropriate Comments to Multiple Colleagues and Attempted Witness Tampering

In April 2023, the OIG issued an investigative summary which found the investigation did not substantiate the initial allegation regarding sexual misconduct. The OIG investigation did find that the AUSA had made and sent inappropriate sexually oriented comments and messages to

multiple colleagues, in violation of DOJ policy. The OIG investigation also found that the AUSA had attempted to tamper with a witness during the OIG's investigation, in violation of federal law and DOJ policy.

Investigative Summary: Findings of Misconduct by a Federal Bureau of Investigation Program Analysis Officer for Sexual Harassment, Unprofessional Conduct, and Lack of Candor to the OIG, and by a then FBI Unit Chief for Failure to Report an Allegation of Sexual Harassment

In June 2023, the OIG issued an investigative summary that substantiated the allegation that the Program Analysis Officer had engaged in sexual harassment and unprofessional conduct, which included, among other things, making sexually suggestive comments towards colleagues and grabbing or slapping the buttocks of four co-workers without their permission, in violation of state and federal law and FBI and DOJ policy. The OIG investigation also substantiated the allegation that the then Unit Chief had failed to report an allegation of sexual harassment by the Program Analysis Officer, in violation of FBI policy. The OIG investigation further found that the Program Analysis Officer lacked candor during an OIG interview, in violation of FBI policy.

Management Advisory Memorandum: Recommendation That the ATF Add to Its Existing Schedule B Policies, Practices, Guidance, and Training a Policy That Specifically Addresses the Recruitment of Friends and Relatives

The purpose of this memorandum was to advise the ATF of concerns the OIG identified regarding a lack of clear procedures, policies, guidance, and training concerning the ATF's Schedule B recruitment process for Special Agents. In December 2022, the OIG issued the Management Advisory Memorandum recommending that the ATF add to its existing Schedule B policies, practices, guidance, and training a policy that specifically addresses the recruitment of friends and relatives to ensure that ATF's recruitment policies and practices are consistent with, and adequately notify ATF employees of, applicable merit-based hiring principles and federal ethics regulations.

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

In December 2022, the OIG issued a report which found that female New Agent Trainees received a disproportionate number of performance citations and were dismissed at rates higher than their overall representation, a substantial number of women reported inappropriate behavior and inconsistent instructor evaluations of trainees based on gender, and few women served in tactical instructor roles. The OIG made seven recommendations to improve the factors that affect gender equity at the FBI Academy, and the FBI agreed with all of them.

Ongoing Work:

Former Prison Guard Arrested for Sexual Abuse of Inmates

On January 25, 2023, a former BOP Correctional Officer previously assigned to the Federal Detention Center in Honolulu, Hawaii, was arrested following an Indictment charging him with 11 counts of sexual abuse of a ward and six counts of sexual abuse. According to the Indictment, from in or about April 2017 through in or about May 2018, Rivera engaged in multiple sexual acts with one inmate using threats and engaged in sexually abusive conduct with two additional inmates who were at the time in official detention and under his custodial, supervisory, and disciplinary authority. The investigation is being conducted by the OIG's Los Angeles Field Office with assistance from the FBI Honolulu Field Office.

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.

8. Whistleblower Program

Whistleblowers perform a critical role when they bring forward evidence of wrongdoing, and they should never suffer reprisal for doing so. 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 be submitted directly to the [OIG Hotline](#).

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 Office of Special Counsel, other agencies, and non-governmental organizations on relevant matters.

During this reporting period, the DOJ OIG Whistleblower Protection Coordinator participated in an OIG community event to educate OIG employees about their whistleblower rights and protections, and the role of the Whistleblower Protection Coordinator. Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed this event in response to the congressional passage of Section 5204 of the FY 2023 National Defense Authorization Act, which requires CIGIE and the OIG Whistleblower Protection Coordinators to ensure that all OIG employees are fully informed about their whistleblower rights and protections. Recognizing the importance of this requirement, the event provided information to the OIG community about the role of the Integrity Committee in assessing allegations of misconduct by Inspectors General and other senior OIG personnel and the role of Whistleblower Protection Coordinators in educating OIG personnel about their rights and protections. Congress recognized, and the community reinforced, the need for Whistleblower Protection Coordinators to not only educate agency employees, but also to empower OIG employees to make protected disclosures when necessary. It is critical that OIGs uphold and promote the same whistleblower rights and protections as the agencies they oversee.

The table below, pulled from our *Semiannual Report to Congress*, presents important information.

October 1, 2022–March 31, 2023

Employee complaints received	606
Employee complaints opened for investigation by the OIG	114
Employee complaints that were referred by the OIG to the components for investigation	313
Employee complaint cases closed by the OIG	115

9. Congressional Testimony

The Inspector General testified before Congress on the following occasions:



- Statement of Michael E. Horowitz Chair, Pandemic Response Accountability Committee Inspector General, U.S. Department of Justice before the U.S. Senate Committee on Homeland Security & Governmental Affairs Emerging Threats and Spending Oversight Subcommittee concerning “Examining Federal COVID-era Spending and Preventing Future Fraud” on [November 14, 2023](#).
- Statement of Michael E. Horowitz Inspector General, U.S. Department of Justice before the U.S. House of Representatives Committee on Appropriations Subcommittee on Crime and Federal Government Surveillance concerning “Fixing FISA: How a Law Designed to Protect Americans Has Been Weaponized Against Them” on [April 27, 2023](#).
- Statement of Michael E. Horowitz Inspector General, U.S. Department of Justice before the U.S. House of Representatives Committee on Appropriations Subcommittee on Commerce, Justice, Science and Related Agencies concerning “The Department of Justice Office of the Inspector General’s Fiscal Year 2024 Budget Request” on [March 23, 2023](#).
- Statement of Michael E. Horowitz Chair, Pandemic Response Accountability Committee Inspector General, U.S. Department of Justice before the U.S. House of Representatives Committee on Ways & Means concerning “Fraud in Federal Unemployment Insurance Programs” on [February 8, 2023](#).
- Statement of Michael E. Horowitz Chair, Pandemic Response Accountability Committee Inspector General, U.S. Department of Justice before the U.S. House of Representatives Committee on Oversight and Accountability concerning “Federal Pandemic Spending: A Prescription for Waste, Fraud, and Abuse” on [February 1, 2023](#).
- Statement of Michael E. Horowitz Inspector General, U.S. Department of Justice before the U.S. Senate Committee on Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations concerning “Sexual Abuse of Female Prisoners in the Custody of the Federal Bureau of Prisons” on [December 13, 2022](#).

E. Challenges

The OIG must confront a variety of internal and external challenges that affect its work and impede progress towards achieving 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.

Furthermore, the limitation on the OIG's jurisdiction has been a challenge for the OIG and 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, a distinction not made in other federal agencies and a limitation not imposed on any other OIG. This duality presents a challenge to the Department as well as to the OIG because of the effect it has on stakeholders' and the public's confidence in the Department's ability to treat its personnel evenhandedly.

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. The length of time it takes to conduct more complex audits, investigations, and reviews is directly impacted by the number of experienced personnel the OIG can devote to these critical oversight activities. As a result, the OIG is requesting a program enhancement to support additional personnel to expand its capacity for oversight across the Department's national security programs and operations, oversight of emerging technologies and information technology (IT) vulnerabilities, and to establish a routine inspections program. The OIG is also requesting program enhancements to continue to modernize its IT and cybersecurity posture.

In addition, since FY 2015, Congress has transferred \$10 million annually to the OIG for oversight and auditing of CVF-funded victim service programs. Because DOJ has a limited capacity for grant monitoring, the OIG plays an important role in detecting and deterring waste, fraud, and abuse in programs designed to improve how crime victims receive the support and assistance they need. Over the last 8 years, the OIG has built a robust victim-centered oversight program that dedicates approximately 45 OIG personnel (almost 9 percent of the OIG workforce) to help ensure CVF funding is effectively and appropriately managed. The loss of \$10 million in CVF funding would have devastating consequence therefore the FY 2025 budget request includes \$5 million in our direct appropriation base for CVF oversight and provides the other \$5 million through the status-quo mechanism of a transfer from the CVF.

II. Summary of Program Changes

Item Name	Description	Pos.	FTE	Dollars (\$000)	Page
Civil Rights Violations, Cybercrime, and Fraud Investigations	The OIG requests a program enhancement of \$1.889 million to support its efforts in conducting complex criminal investigations and investigate highly sensitive matters relating to allegations of waste, fraud, abuse, and misconduct involving DOJ programs and personnel.	8	8	\$ 1,889.0	31
Cybersecurity and Technology Enhancement	The OIG requests a program enhancement of \$4.865 million focusing on three crucial areas: (1) modernizing the OIG's mission and business processes through the deployment of software automation, (2) enhancing the OIG's security footprint and eDiscovery capabilities by implementing Artificial Intelligence (AI) and Machine Learning, and (3) updating and maintaining the OIG's Body Worn Camera (BWC) Program.	0	0	\$ 4,865.0	35
National Security Programs and Operations Oversight	The OIG requests positions to boost our capacity for rigorous oversight across the Department's national security programs and operations. This includes critical domains such as counterintelligence, counterterrorism, and cyber, where increased scrutiny is paramount in this rapidly evolving security environment.	8	8	\$ 1,820.0	38
Establish OIG's IT Security & Emerging Technology Oversight Unit	The OIG requests resources to create an IT Security and Emerging Technology Oversight Unit within the OIG's Audit Division and hire or contract staff with technical expertise in emerging technologies and IT vulnerability mitigation. This will allow the OIG to better align and enhance our oversight of the Department's Strategic Framework for FY 2022-2026 in combating the ever-evolving threats in the cyber environment, including ransomware attacks and cyber supply chain risks, as well as in overseeing the Department's increasing use of artificial intelligence and other machine learning technologies.	4	4	\$ 1,513.0	43
Cybersecurity and Information Technology Division Enhancement	The OIG requests funding for three crucial areas: (1) enhancing the OIG's cybersecurity posture, (2) modernizing the OIG's business processes through the deployment of modern tools and automated applications, and (3) deployment of a classified case management system.	4	4	\$ 1,885.0	48

Prison Inspections Program Enhancement	The OIG requests funding for positions to enhance its efforts to assess and help the BOP improve the conditions of confinement in federal prisons. Specifically, the OIG would like to expand its capacity to conduct unannounced, routine inspections of the 122 nationwide BOP prisons.	8	8	\$ 1,570.0	53
Total		32	32	\$ 13,542.0	

III. Appropriations Language and Analysis of Appropriations Language

Office of Inspector General

For necessary expenses of the Office of Inspector General, [~~\$151,636,000~~] *\$166,590,000* 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, [~~2025~~] *2026*.

Provided, That notwithstanding section 1402(d) of such Act, of the amounts available from the Fund for obligation: (1) [~~\$10,000,000~~] *\$5,000,000* 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

Since FY 2015, Congress has transferred \$10 million annually to the OIG for CVF oversight. The FY 2025 budget request includes \$5 million in our direct appropriation base for CVF oversight and provides the other \$5 million through the status-quo mechanism of a transfer from the CVF. The transfer language is in Sec. 510.

IV. Program Activity Justification

A. Audits, Inspections, Investigations, and Reviews

Program Increases

OIG	Direct Pos.	Direct FTE	Amount
2023 Enacted	560	516	\$149,000
2024 Continuing Resolution	546	521	\$149,000
Adjustments to Base and Technical Adjustments	0	0	\$9,048
2025 Current Services	546	521	\$158,048
2025 Program Increases	32	32	\$13,542
2025 Request	578	553	\$171,590
Total Change 2024-2025	32	32	\$22,590

All references in this document and tables to an FY 2024 Continuing Resolution are to an FY 2024 Annualized Continuing Resolution.

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												
Decision Unit: OIG/Audits, Inspections, Investigations, and Reviews												
RESOURCES (\$ in thousands)			Target		Actual		Target		Changes		Requested (Total)	
			FY 2023		FY 2023		FY 2024 CR		Current Services Adjustments and FY 2025 Program Changes		FY 2025 Request	
Total Costs and FTE <small>(Reimbursable: FTE are included, but costs are bracketed and not included in totals)</small>			FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000
			580	\$149,000 [\$15,599]	536	\$149,000 [\$15,599]	541	\$149,000 [\$15,921]	34	\$22,590 [\$168]	575	\$171,590 [\$15,959]
TYPE	STRATEGIC OBJECTIVE	PERFORMANCE	FY 2023		FY 2023		FY 2024 CR		Current Services Adjustments and FY 2025 Program Changes		FY 2025 Request	
APG Measure:	1.2	Promote Good Government	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000	FTE	\$000
			580	\$149,000 [\$15,599]	536	\$149,000 [\$15,599]	541	\$149,000 [\$15,921]	34	\$22,590 [\$168]	575	\$171,590 [\$15,959]

		PERFORMANCE MEASURE TABLE						
		Decision Unit:						
Strategic Objective		Performance Measures	FY 2022	FY 2023	FY 2023	FY 2024	FY 2025	
			Actual	Target	Actual	Target	Target	
1.2	Performance Measure	Number of Cases Opened per 1,000 DOJ employees: Fraud	0.19	*	0.21	*	*	
1.2	Performance Measure	Number of Cases Opened per 1,000 DOJ employees: Bribery	0.05	*	0.08	*	*	
1.2	Performance Measure	Number of Cases Opened per 1,000 DOJ employees: Rights Violations	0.14	*	0.12	*	*	
1.2	Performance Measure	Number of Cases Opened per 1,000 DOJ employees: Sexual Crimes	0.12	*	0.16	*	*	
1.2	Performance Measure	Number of Cases Opened per 1,000 DOJ employees: Official Misconduct	0.7	*	0.65	*	*	
1.2	Performance Measure	Number of Cases Opened per 1,000 DOJ employees: Theft	0.04	*	0.06	*	*	

1.2	Performance Measure	Percentage of BOP Investigations closed or referred for prosecution within 6 months of being opened	93%	75%	95%	75%	75%
1.2	Performance Measure	Number of closed Investigations substantiated*	166	*	148	*	*
1.2	Performance Measure	Arrests *	80	*	67	*	*
1.2	Performance Measure	Convictions *	68	*	84	*	*
1.2	Performance Measure	Administrative Actions *	129	*	175	*	*
1.2	Performance Measure	Response to Customer Surveys: Report completed in a timely manner	93%	90%	100%	90%	90%
1.2	Performance Measure	Response to Customer Surveys: Issues were sufficiently addressed	98%	90%	100%	90%	90%
1.2	Performance Measure	Integrity Briefings/Presentations to DOJ employees and other stakeholders	183	70	240	70	70
1.2	Performance Measure	DOJ employees and stakeholders at Integrity Briefings	3,291	3,000	5,510	3,000	3,000
1.2	Performance Measure	Audit assignments initiated	108	99	147	99	99
1.2	Performance Measure	E&I assignments initiated	4	*	2	4	4
1.2	Performance Measure	Percent of CSITAO* resources devoted to security reviews of major DOJ information systems security reviews of major DOJ information systems	91%	80%	93%	80%	80%
1.2	Performance Measure	Percent of internal DOJ audit reports that assess component performance measures	79%	60%	89%	65%	65%

1.2	Performance Measure	Percentage of E&I assignments opened and initiated during the fiscal year devoted to Top Management Challenges	100%	70%	100%	70%	70%
1.2	Performance Measure	Percent of direct resources devoted to audit products related to Top Management Challenges, and GAO and JMD-identified High-Risk Areas	99%	85%	90%	85%	85%
1.2	Performance Measure	Audit assignments completed	116	99	112	99	99
1.2	Performance Measure	E&I assignments completed	6	*	8	4	4
1.2	Performance Measure	Percent of Audit resources devoted to reviews of contracts and contract management	14%	5%-8%	15%	5%-8%	5%-8%
1.2	Performance Measure	Components receiving information system audits	11	6	11	6	6
1.2	Performance Measure	Percent of products issued to the Dept. or other Federal entities containing significant findings or information for management decision-making by Audit	100%	90%	100%	90%	90%
1.2	Performance Measure	Percent of products issued to the Dept. or other Federal entities containing significant findings or information for management decision-making by E&I	100%	86%	100%	86%	86%
1.2	Performance Measure	Percent of internal DOJ (E&I) reviews to be provided to the IG as a working draft within 12 months	83%	35%	50%	35%	35%
1.2	Performance Measure	Percent of grant, CODIS, equitable sharing, and other external audits to be completed in draft within 8 months	53%	40%	66%	40%	40%
1.2	Performance Measure	Percent of internal DOJ audits to be provided to the IG as a working draft within 13 months	97%	60%	92%	60%	60%

* Indicators for which the OIG only reports actuals.

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 top management and performance challenges.

VI. Program Increases by Item

Item Name: Civil Rights Violations, Cybercrime, and Fraud Investigations				
Strategic Goal(s) & Objective(s):	Strategic Goal 1: Uphold the Rule of Law Objective 1.1: Protect Our Democratic Institutions Objective 1.2: Promote Good Government Strategic Goal 2: Keep Our Country Safe Objective 2.1: Protect National Security			
Organizational Program:	OIG			
Program Increase:	Positions 8	Agt/Atty 8/0	FTE 8	Dollars \$1,889,000
	Equipment/software/services:		Dollars \$0.00	
Total Request of Increase:	\$1,889,000			

1. Description of Item

As part of the OIG’s ongoing efforts to promote trust and accountability in law enforcement, combat public corruption, and protect civil rights, the Investigations Division (INV) is requesting a program increase of **\$1.889 million**. INV has primary responsibility for conducting complex criminal investigations and investigates other highly sensitive administrative matters relating to allegations of waste, fraud, abuse, and misconduct involving DOJ programs and personnel.

The additional funding will enable INV to hire eight Special Agents in multiple office locations across the country. The resources will enable INV to broaden its oversight by opening more investigations involving: official corruption, including expansion of our capability to handle cases involving the Federal Bureau of Prisons (BOP); civil rights violations committed by DOJ law enforcement personnel; and fraud by recipients of grants and contracts funded by DOJ. The resources will also enhance INV’s ability to keep pace with the increasing number of digital evidence items that are associated to the majority of our investigations, and the analysis of the digital evidence. We estimate that these additional resources will allow INV to open between 55-65 additional cases.

2. Justification

The Attorney General’s strategic goals and objectives specifically address the importance of maintaining a safe and humane prison system (DOJ Strategic Goal 5, Objective 5.2). Law enforcement is instrumental in protecting the civil rights of individuals equally (DOJ Strategic

Goal 3, Objective 3.3). INV has investigated numerous civil rights violations involving physical abuse, excessive use of force, and sexual abuse of inmates committed by DOJ personnel inside the prison setting. For example, INV is conducting 10 investigations of staff misconduct related to sexual abuse of inmates at the Federal Correctional Institution in Dublin, CA. To date, these investigations have resulted in charging documents for five subjects, two of whom have pled guilty. One of the indicted subjects was the Warden of the prison and the others were Correctional Officers who allegedly abused the trust and authority placed on them to oversee the safety of the institution and the inmates. INV has also investigated numerous BOP personnel for the introduction of contraband into a prison. For example, a BOP chaplain was sentenced to 40 months imprisonment for accepting approximately \$52,000 in bribe payments for smuggling drugs (Suboxone, synthetic cannabinoids, and marijuana), cell phones, tobacco, and other contraband into the prison. Many of INV's cases involve the introduction of drugs into a prison that leads to enhanced security risks, ongoing drug trafficking activities, and sometimes overdoses resulting in the death of inmates (DOJ Strategic Goal 2, Objective 2.5). In FY 2021, INV opened 42 introduction of contraband cases equaling only 21 percent of the total number of complaints received. The OIG is currently developing an interdisciplinary team to focus on official corruption and systemic misconduct within the BOP, which we expect to generate additional investigations. The resources requested will enable the OIG to take on more of the matters that we currently refer to BOP for it to handle.

In addition to official corruption and misconduct inside prisons, the OIG seeks additional resources for official corruption investigations by other law enforcement personnel. Due to resource limitations, in FY 2021 INV was able to open only 9 physical abuse/excessive use of force cases equaling only 1.5 percent of the total number of such complaints received, and 20 sexual abuse cases equaling 9 percent of such complaints received. The number of physical abuse complaints received by INV has increased steadily over 5 years, resulting in a 64 percent increase from FY 2016 to FY 2021. Although the number of sexual abuse complaints have fluctuated over the past 5 years, it is essential that INV opens more sexual abuse cases to align with the Department's goals. It is crucial that these types of civil rights violations are investigated to ensure that the Department is promoting integrity in law enforcement. Additional resources to focus on these types of investigations will allow the OIG to keep up with the increased number of these troubling cases.

INV's Cyber Investigations Office (Cyber) conducts computer and mobile device forensic examinations on hundreds of pieces of digital evidence annually, which includes computers, hard drives, cell phones, tablets and other electronic media. These examinations are crucial to the discovery of evidence of official misconduct, which enables DOJ personnel to be held accountable for their actions. Over the past several years, the pieces of evidence submitted by agents to Cyber for extraction have steadily increased and more than doubled over the last five years.

Digital forensic capabilities have become an integral part of the OIG's investigative work and based on this consistent trend we can expect that the OIG's reliance on these capabilities will continue to increase over time. Additionally, more people keep electronic records and communicate by electronic devices that also add to the complexity of each investigation. The number of electronic documents and communications in today's cases far exceed the number of hard copy documents in cases worked even 5 or 10 years ago. Furthermore, Cyber not only conducts forensic exams for all of the OIG Divisions but is often asked to assist other agencies without this capability putting a further strain on our limited resources. Cyber forensic

examinations can take many hours, days, or weeks just for one device let alone multiple devices for one investigation. Subsequent to Cyber conducting the forensic exam/extraction on the device, the results must be analyzed. The analysis of the voluminous records and communications is completed by a field agent outside of Cyber, which puts a strain on the agent's time and their ability to work on other critical investigations. The additional agents strategically placed throughout the country will assist INV to keep up with the steady volume increase while allowing us to open other complex matters.

Throughout the federal government, procurement has historically been prone to fraud and waste. INV has been successful in combating corruption, financial crime, and fraud (DOJ Strategic Goal 4, Objective 4.2) involving DOJ programs and personnel. Any time taxpayer funds are distributed to third parties, such as grantees and contractors, there is an increased risk of mismanagement and misuse. In FY 2021 we opened 22 cases associated to contract, grant, and healthcare fraud equaling 31 percent of the total complaints we received related to these programs. Combating fraud in DOJ programs is extremely important and contributes to saving taxpayer dollars. Moreover, INV's investigative activities have already had a significant return on investment for the taxpayer. In the OIG's Semiannual Report to Congress for the first half of FY 2022, the INV Division has already had monetary results totaling over \$9M and has consistently had monetary results in the multi-millions: FY 2021 \$15M (pandemic entire year); FY 2020 \$2.8M (pandemic during second half); FY 2019 \$68M; FY 2018 \$81M; and FY 2017 \$27M. With additional resources, the OIG's efforts to combat fraud would enable the opening of additional cases, and thereby hold accountable more of those who seek to cheat to obtain taxpayers' dollars.

3. Current State and Impact on Performance

At current staffing levels, the rapid increase and expected further increase in the number of cases involving civil rights violations, sexual abuse, introduction of contraband, fraud, and cybercrime inevitably reduces the critical investigations that INV can undertake in a timely fashion. Over the past several years, INV has also seen a steady increase in the complexity of cases, which further strains existing resources and generally requires more time to complete. Currently, 39 percent of INV's open cases have multiple subjects. This requires the assigned agent to sometimes run multiple investigations within the same case or have other agents across the country assist with the case. The additional resources will allow INV to open between 55-65 additional cases at any given time and enhance the timeliness for completing more complex cases. The OIG takes very seriously its commitment to taxpayers, Congress, and other stakeholders to continue providing timely and quality investigations, results, and reports. This request will significantly enhance the OIG's ability to provide the high-level of quality work that stakeholders expect.

Funding
Civil Rights Violations, Cybercrime, and Fraud Investigations
(Dollars in Thousands)

1. Base Funding

<i>FY 2023 Enacted</i>				<i>FY 2024 Continuing Resolution</i>				<i>FY 2025 Current Services</i>			
Pos	Agt/Atty	FTE	Amount (\$000)	Pos	Agt/Atty	FTE	Amount (\$000)	Pos	Agt/Atty	FTE	Amount (\$000)
175	146	175	\$39,487.0	175	146	175	\$41,540.3	175	142	175	\$42,371.2

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2025 Request (\$000)	Positions Requested	Full Year Modular Cost per Position (\$000)	Annualizations (\$000)			
				2 nd Year	3 rd Year	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Special Agents (1811)	\$1,888.8	8	\$236.1	\$220.50	\$232.50	-\$15.6	\$12.0
Total Personnel	\$1,888.8	8	\$236.1	\$220.50	\$232.50	-\$15.6	\$12.0

3. Total Request for this Item

Category	Positions			Amount Requested (\$000)			Annualizations (\$000)	
	Count	Agt/Atty	FTE	Personnel	Non-Personnel	Total	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Current Services	175	142	175	\$42,371.2	\$0.00	\$42,371.2	N/A	N/A
Increases	8	8	8	\$1,888.8	\$0.00	\$1,888.8	(\$124.8)	\$96.0
Grand Total	183	150	183	\$44,260.0	\$0.00	\$44,260.0	(\$124.8)	\$96.0

4. Affected Crosscuts – Civil Rights

Item Name: Cybersecurity and Technology Enhancement				
Strategic Goal(s) & Objective(s):	Strategic Goal 1: Uphold the Rule of Law Objective 1.1: Protect Our Democratic Institutions Objective 1.2: Promote Good Government Strategic Goal 2: Keep Our Country Safe Objective 2.4: Enhance Cybersecurity and Fight Cybercrime			
Organizational Program:	OIG			
Program Increase:	Positions 0	Agt/Atty 0/0	FTE 0	Dollars \$0
	Equipment/software/services:		Dollars \$4,865,000	
Total Request of Increase:	\$4,865,000			

1. Description of Item

In an effort for the OIG to meet the DOJ’s goals of upholding the rule of law and keeping our country safe and to continue to promote integrity, efficiency, accountably, and good government through robust independent oversight, the OIG requires a program enhancement of **\$4.865 million** to continue to modernize its information technology (IT) and cybersecurity posture. The program enhancement focuses on three crucial areas: (1) modernizing the OIG’s mission and business processes through the deployment of software automation, (2) enhancing the OIG’s security footprint and eDiscovery capabilities by implementing Artificial Intelligence (AI) and Machine Learning, and (3) updating and maintaining the OIG’s Body Worn Camera (BWC) Program.

2. Justification

To promote transparency and continually assess internal processes and practices to maximize the efficiency and economy of operations, the OIG requests the specific program enhancements described below to support its ongoing IT modernization initiative and achieve its mission to promote integrity, efficiency, and accountability within the DOJ.

(1) Modernizing OIG Processes - \$2.76M

As the OIG mission continues to grow, there is an immediate need to provide tools and services to improve and support productivity to enhance the overall OIG mission. This program enhancement would allow the OIG to develop and implement innovative, scalable, digital services transforming the current manual OIG business and mission processes into a modern, flexible architecture that maximizes the use of limited resources. The OIG seeks to adopt current DOJ capabilities such as an IT service management platform to reengineer current IT manual processes such as incident and problem management, configuration and change management,

knowledge management, and service catalog and request management. Additionally, the OIG would replace its current manual financial process and implement the DOJ's digital financial management platform which would allow the OIG to streamline all financial processes between the agencies. In the absence of this program enhancement, the OIG will continue to need additional support personnel to manage current manual business processes and the OIG will confront continuing difficulties in meeting its current mission requirements from a technical perspective due to a growing gap between the OIG's and the DOJ's technical services environment.

(2) Implementing Artificial Intelligence (AI) and Machine Learning - \$1.99M

AI and machine learning technologies provide faster and more accurate data gathering and processing, enabling agencies to focus on more complex and long-term issues. Additionally, they help agencies track and manage large amounts of data to analyze in real time for anomalies and threats. In 2021, the Federal Government saw an immediate need to increase security around government IT infrastructures to safeguard data and networks. Additionally, the OIG opened 231 investigations and issued 51 reports requiring extensive eDiscovery resources. To meet these mission requirements, the OIG has a need to develop more robust eDiscovery capabilities while enhancing its IT security footprint. This program enhancement allows the OIG to develop an AI and machine learning program to harden the OIG IT infrastructure from cyber threats. Implementing this program allows the OIG to defend against cyber threats through utilizing automation to drive accuracy and acceleration in early threat detection. Additionally, this program enhancement provides cloud-based AI services to build cognitive intelligence into OIG applications for eDiscovery purposes which would decrease the OIG's time to issue, complete, and close reports. While this program enhancement will meet the immediate needs described above, it will be scalable to provide future resources to the OIG Office of Data Analytics and Cybersecurity Investigations, strengthening the OIG's future mission capabilities.

(3) Maintain the Body Worn Camera Program – \$115K

Following a series of incidents involving the alleged use of excessive force by law enforcement in the summer of 2020, there were protests across the country related to police brutality and calls for widespread reform, some of which were followed by the release of video footage that appeared to contradict official accounts of events. BWCs can be an effective tool to enhance law enforcement transparency and accountability and help build public trust. In FY 2022, the OIG implemented a BWC Program in response to these events. The OIG is dedicated to upholding the Rule of Law and ensuring the transparency and accountability of its law enforcement agents and this program enhancement allows the OIG to maintain software licenses necessary for the technical aspects of the BWC Program, address growing data storage needs from operation of the program, and add enhancements to its BWC Program over time.

3. Current State and Impact on Performance

Without the enhancements noted above, the OIG will be deficient in meeting rising cybersecurity demands on the IT infrastructure, remaining agile to respond to cyber threats, or maintaining the current OIG mission pace. 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 expanding mission needs and current technology capabilities within the OIG's IT infrastructure.

**Cybersecurity and Technology Enhancement
(Dollars in Thousands)**

1. Base Funding

<i>FY 2023 Enacted</i>				<i>FY 2024 Continuing Resolution</i>				<i>FY 2025 Current Services</i>			
Pos	Agt/Atty	FTE	Amount (\$000)	Pos	Agt/Atty	FTE	Amount (\$000)	Pos	Agt/Atty	FTE	Amount (\$000)
28	0	28	\$17,770.2	28	0	28	\$19,560.9	28	0	28	\$20,017.0

2. Non-Personnel Increase Cost Summary

Non-Personnel Item	FY 2024 Request (\$000)	Unit Cost (\$000)	Quantity	Annualizations (\$000)	
				FY 2025 (Net change from 2024)	FY 2026 (Net change from 2025)
Modernizing OIG Processes – IT Services, Budget and Financial Processes	\$2,760.0	N/A	1	-\$1,810.0	\$19.0
Implementing AI and Machine Learning	\$1,990.0	N/A	1	-\$500.0	\$30.0
Body Worn Camera Program	\$115.0	N/A	1	\$2.3	\$4.6
Total Non-Personnel	\$4,865.0	N/A	1	-\$2,307.7	\$53.6

3. Total Request for this Item

Category	Positions			Amount Requested (\$000)			Annualizations (\$000)	
	Count	Agt/Atty	FTE	Personnel	Non-Personnel	Total	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Current Services	28	0	28	\$7,663.0	\$12,353.0	\$20,016.0	N/A	N/A
Increases	0	0	0	\$0.00	\$4,865.0	\$4,865.0	-\$2,307.7	\$53.6
Grand Total	28	0	28	\$7,213.4	\$21,126.8	\$28,340.2	-\$2,307.7	\$53.6

4. Affected Crosscuts – Cybersecurity

Item Name: Increase OIG’s Capacity to Oversee DOJ’s National Security Programs and Operations				
Strategic Goal(s) & Objective(s):	Strategic Goal 1: Uphold the Rule of Law Objective 1.1: Protect Our Democratic Institutions Objective 1.2: Promote Good Government Strategic Goal 2: Keep Our Country Safe Objective 2.1: Protect National Security			
Organizational Program:	OIG			
Program Increase:	Positions 8	Agt/Atty 0/1	FTE 8	Dollars \$1,820,300
	Equipment/software/services:		Dollars \$0.00	
Total Request of Increase:	\$1,820,300			

1. Description of Item

The Department requests a program increase of **\$1,820,300** for eight positions to boost the OIG’s capacity for rigorous oversight across the Department’s national security programs and operations. This includes critical domains such as counterintelligence, counterterrorism, and cyber, where increased scrutiny is paramount in this rapidly evolving security environment. This request aligns with the Department’s Strategic Plan for FYs 2022-2026 which includes, but is not limited to, efforts to: (1) deter, disrupt, and prosecute terrorist threats; (2) protect civil liberties; (3) counter cyber-based national security threats; and (4) safeguard sensitive assets. If authorized, the requested positions will be allocated between the Oversight and Review Division and the Audit Division’s Regional Audit Offices, enabling the OIG to conduct additional oversight through an additional one to two audits or reviews of the Department’s critical and frequent highly classified national security activities each year. These positions include five auditors, two program analysts, and one attorney who will be directly responsible for conducting the audits and reviews.

2. Justification

National security has been among the Department's top priorities dating back to the attacks of September 11, 2001. The Department continues to face immense challenges in countering terrorism, mitigating insider threats, and defending the country from nation states and criminal actors looking to gain a political, military, or economic advantage. To effectively mitigate these national security threats, the Department relies on a vast array of components, such as the Criminal Division, Drug Enforcement Administration (DEA), Federal Bureau of Investigation (FBI), Justice Management Division, National Security Division, and U.S. Attorneys’ Offices across the country. Auditing or reviewing a single national security program within one of these entities requires substantial OIG resources, and the resource need increases when a program

involves more than one Department component. Further, as the Department and its components increase their resources in national security programs and operations, it is incumbent upon the OIG to ensure we maintain sufficient coverage of these expanded areas. For instance, in FY 2024 the FBI alone requested approximately \$81 million in program enhancements for national security-related programs, which is half of the total funding requested that year by the OIG in its entirety.

The OIG has demonstrated significant value in providing recommendations to improve the Department's national security programs and ensuring accountability in operations that were largely obscured from essential public evaluation and scrutiny. The OIG continually evaluates the Department's national security programs to identify high-risk areas where the OIG's oversight can play a crucial role in ensuring Department operations and tactics are (1) performed effectively to best ensure the nation's security and (2) in accordance with laws and regulations to protect civil rights and personal liberties.

However, given the OIG's oversight responsibilities throughout the Department's vast and varied components and programs, we are unable to allocate sufficient resources to address a significant portion of the Department's highest risk national security programs and operations. With this additional enhancement, we will be better positioned to keep pace with and more promptly initiate oversight projects identified through the OIG's risk assessment processes. For instance, we would be able to commence work on important and time-sensitive projects associated with Department programs and operations, including those that support Ukraine's efforts to combat Russian aggression; the use of national security and counterintelligence sensitive investigative authorities, such as those authorized by the Foreign Intelligence and Surveillance Act (FISA); management and oversight of sensitive off-site locations; responses to national security cyber threats; efforts to safeguard research and development grants from foreign influence, espionage, and theft; and the access to and use of private data and personal identifying information in national security and counterintelligence programs. With the additional requested resources, the OIG will be able to conduct oversight in one or more these important areas.

For over 20 years, national security has been identified by the OIG as a top management and performance challenge, and we have delivered significant and valuable oversight of certain risks and challenges. This was particularly evidenced in the OIG's *Review of Four FISA Applications and Other Aspects of the FBI's Crossfire Hurricane Investigation* and the *Audit of the FBI's Execution of its Woods Procedures for Applications Filed with the FISA Court Relating to U.S. Persons*. These efforts required over 25 OIG personnel from multiple OIG Divisions, which far exceeds the OIG's capacity to routinely dedicate resources to national security issues given its limited resources and overall oversight responsibilities. The latter report confirmed that problems with the implementation of the FBI's factual accuracy review procedures ("Woods Procedures") were not isolated to the FISA applications examined in our Crossfire Hurricane review. This project required the quick assembly of a large team that was deployed to a sample of eight different, geographically dispersed FBI field offices. In each of these instances the need to surge resources to fully staff these projects negatively impacted the OIG's ability to conduct needed oversight in other national security and non-national security areas alike. The additional requested resources will enable the OIG to become more agile in addressing national security matters as they arise, as well as improve our ability to maintain a consistent oversight presence in the Department's national security programs and operations without compromising our oversight of the rest of the Department's high-risk operations.

Reauthorization of Section 702 of the FISA Amendments Act—scheduled to expire on December 31, 2023—is a top Department priority. Specifically, the Attorney General described Section 702 as “an indispensable tool for protecting American national security.” However, the Department faces challenges in assuring Congress and the American public that the safeguards built into Section 702 minimize the collection, retention, and dissemination of information on U.S. persons. In March 2023, the House Permanent Select Committee on Intelligence announced the formation of a bipartisan FISA 702 Working Group that will consider reforms to improve the legislation and protect American civil liberties from cases of misuse and exploitation. OIG oversight of the implementation of such reforms and the Department’s compliance with added protections will be an important element of the public’s confidence in the Department’s actions in this sensitive area and the OIG remains fully committed to overseeing Department compliance with any new resulting legislation. However, to best maintain adequate FISA-related oversight while also continuing our important work in other non-FISA national security programs and operations, the OIG will need the requested additional personnel resources to accomplish such oversight in a timely and efficient manner.

The OIG’s national security oversight work often results in the discovery of issues and risks that may impact non-national security programs and operations. For example, our *Audit of the FBI’s National Security Undercover Operations* found that the time to approve requested Attorney General exemptions for undercover operations was excessive, causing delays to those operations, and that those requests were not tracked effectively. During this same audit, due in part to limited resources, the OIG was not able to immediately pursue some complex and expansive issues we identified with the FBI’s use of tradecraft to protect its investigations, operations, and personnel. Instead, the OIG had to delay its work in this area by more than a year until we were able to start our subsequent *Audit of the FBI’s Efforts to Respond to Changing Operational Technologies*. This audit is ongoing and has preliminarily identified concerns that may go beyond the FBI’s national security operations. If additional OIG personnel were available in such instances, the OIG would have been in a better position to expand the scope of the review to other relevant components, providing a more timely and effective service to the Department and the nation.

Moreover, OIG audits and reviews increasingly encounter activities that blur the boundaries between criminal and national security threats. This dynamic is evident in the OIG’s ongoing *Audit of the Department of Justice’s Strategy to Combat and Respond to Ransomware Threats*, which involves DOJ efforts against both cybercriminals and nation-state actors. Furthermore, because the FBI and DEA are members of the U.S. intelligence community, it may be necessary for audits and reviews to assess compliance with national security requirements, such as during the *Audit of the Department’s Cyber Supply Chain Risk Management Efforts*. Without an increase in OIG staff, we are unable to promptly address these matters as they arise and will be limited in our ability to respond to the steadily increasing workload resulting from public reporting, as well as Department and congressional concerns.

OIG’s national security audits and reviews often involve classified material, up to and including highly classified Top Secret and Sensitive Compartmented Information. As noted above, previously, our capacity to initiate projects involving such material was limited to some degree due to the availability of only three OIG SCIFs, all of which are located within the Washington, D.C. metropolitan area. Congress has already provided the OIG \$1.95 million to build SCIFs in two OIG field locations, with construction commencing in FY 2024. With the planned construction of these SCIFs, we are now in an optimal position to enhance our capacity to

conduct national security oversight throughout OIG regional offices. Furthermore, the OIG intends to design and construct two additional SCIFs in other field locations, expanding national security oversight and reducing the need for staff to travel to access and process highly classified information properly.

3. Current State and Impact on Performance

It is vital that the OIG provides timely and relevant oversight on issues of significance to the Department, Congress, and the American public. National security audits and reviews are resource intensive and compete with other DOJ risks requiring the OIG's attention. The enhancements mentioned above will allow the OIG to expand its ability to conduct agile and continuous oversight of the Department's persistently evolving national security programs and activities, including counterintelligence, counterterrorism, and cyber threats. As it stands, the OIG's national security work is carried out by a small set of highly skilled teams. Despite our expertise and understanding of this domain, competing priorities limit the OIG's ability to provide needed additional oversight of the vast and rapidly evolving scope of the Department's national security programs and operations. With these additional requested resources, the OIG believes it will be in a position to expand its ability to conduct this critically important oversight by one to two national security-related audits or reviews each year.

Funding
National Security Programs and Operations
(Dollars in Thousands)

1. Base Funding

<i>FY 2023 Enacted</i>				<i>FY 2024 Continuing Resolution</i>				<i>FY 2025 Current Services</i>			
Pos	Agt/Atty	FTE	Amount (\$000)	Pos	Agt/Atty	FTE	Amount (\$000)	Pos	Agt/Atty	FTE	Amount (\$000)
61	24	61	\$16.429	61	24	61	\$16.922	61	24	61	\$17.768

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2025 Request (\$000)	Positions Requested	Full Year Modular Cost per Position (\$000)	Annualizations (\$000)			
				2 nd Year	3 rd Year	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Clerical and Office Svcs (0300-0399)	\$423.0	2	\$423.0	\$417.2	\$437.4	-\$5.8	\$20.2
Accounting and Budget (0500-0599)	\$1,103.3	5	\$1,103.3	\$1,090.9	\$1,138.1	-\$12.4	\$34.8
Attorneys (0905)	\$294.0	1	\$294.0	\$296.6	\$310.8	\$2.5	\$14.2
Total Personnel	\$1,820.3	8	\$1,820.3	\$1804.7	\$1,886.3	-\$15.7	\$69.2

3. Total Request for this Item

Category	Positions			Amount Requested (\$000)			Annualizations (\$000)	
	Count	Agt/Atty	FTE	Personnel	Non-Personnel	Total	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Current Services	61	24	61	\$13,348	4,419	\$17,768	N/A	N/A
Increases	8	1	8	\$1,820.3	0	\$1,820.3	\$91.0	\$95.6
Grand Total	69	25	69	\$15,168.3	\$4,419	\$19,588.3	\$979.4	\$1,028.4

4. Affected Crosscuts - National Security

Item Name: Establish OIG’s IT Security & Emerging Technology Oversight Unit				
Strategic Goal(s) & Objective(s):	Strategic Goal 1: Uphold the Rule of Law Objective 1.1: Protect Our Democratic Institutions Objective 1.2: Promote Good Government Strategic Goal 2: Keep Our Country Safe Objective 2.4: Enhance Cybersecurity and Fight Cybercrime			
Organizational Program:	OIG			
Program Increase:	Positions 4	Agt/Atty 0/0	FTE 4	Dollars \$963,100
	Equipment/software/services:		Dollars \$550,000	
Total Request of Increase:	\$1,513,000			

1. Description of Item

The Department requests **\$1,513,000** for four positions and additional resources to enhance its oversight of the Department's high-risk Information Technology (IT) portfolio.

The requested resources will be used to create an IT Security and Emerging Technology Oversight Unit within the OIG's Audit Division and hire or contract staff with technical expertise in emerging technologies and IT vulnerability mitigation. This will allow the OIG to better align and enhance our oversight of the Department's Strategic Framework for FY 2022-2026 in combating the ever-evolving threats in the cyber environment, including ransomware attacks and cyber supply chain risks, as well as in overseeing the Department’s increasing use of artificial intelligence and other machine learning technologies.

2. Justification

In the Department’s efforts to keep the American people safe, it continues to face a multitude of serious and evolving threats from cyber terrorism, cybercrime, and cyber-enabled crime. The world’s reliance on technology continues to grow at an increasing rate and the Department must keep pace with these advances in order to effectively oversee, manage, and protect its IT systems, information management, and data collection capabilities. The Department's total IT spending in FY 2022 was \$3.7 billion, which is a staggering \$1 billion increase from 10 years ago. Moreover, while technology plays an essential supporting role in the Department’s daily workplace activities, the Department also tactically deploys emerging technologies in its national security and law enforcement operations. The use of these tools and capabilities must align with the Department’s moral imperative to uphold the rule of law, keep our country safe, and protect civil rights.

In 2021, the DOJ triaged over 430,000 reported cyber incidents and recently reported that it faces persistent and increasingly sophisticated malicious cyber campaigns that threaten its ability to protect the DOJ's national security and law enforcement missions. The increase in attacks on federal networks and systems highlight the necessity and importance of vigilant oversight to ensure the systems that house government and taxpayer data are not compromised by improper security practices or vulnerabilities that can harm the public trust. The 2020 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 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 eight months and made clear that a successful breach of the Department's networks will threaten to undermine its ability to carry out its mission, as well as risk exposing information that jeopardizes economic, national, and personal security. In addition, the February 2023 ransomware attack on the U.S. Marshals Service highlighted the risk of component systems not deploying the most current IT infrastructure and protections. Both incidents highlight that the Department will continue to be a target for malicious activity. The ever-changing landscape of cyber intrusions, state sponsorship of those intrusions, and the sensitive information contained in the Department's unclassified and classified IT systems make it vital that the OIG grow its capability to oversee the Department's efforts to ensure that its data and systems are secure, and that the Department maintains network resilience.

While the OIG performs statutorily required Federal Information Security Modernization Act (FISMA) audits, FISMA audits primarily address known risks and standard controls in place over IT systems. The OIG seeks to create a complementary IT Security & Emerging Technology Oversight Unit to augment our current IT oversight with positions and resources performing more proactive oversight of the Department's enterprise-wide IT security efforts, such as through the implementation of continuous monitoring of the Department's efforts to identify and address IT security issues through its national security, investigative, and prosecutorial mission.

To accomplish this critical oversight, the OIG needs additional personnel with both IT security experience and those capable of understanding the vulnerabilities that malicious actors could exploit to gain access to Department systems, enabling the OIG to better oversee the Department's practices, more effectively boost efforts for securing its systems and data, and ensuring resiliency against attacks. This funding supports four full-time equivalents, and two contractors with a particular expertise, such as knowledge of a specific programming code, machine learning, or security vulnerability exploitation. With these additional resources, the OIG's oversight work can continue to keep pace with the Department's need to identify vulnerabilities and areas for enhanced internal controls, as well as its efforts to thwart and mitigate the effects of inevitable future attacks, similar in magnitude to SolarWinds.

Emerging technologies continue to pose new issues – whether those technologies are used for unlawful purposes by hostile nation-states and cyber criminals or used by the Department to further its investigations and critical operations. Artificial Intelligence (AI) is just one of these emerging technologies that requires increased oversight. The Department issued its AI Strategy in December 2020 signaling its intent to embrace this transformative technology. However, the use of AI technologies, including facial recognition, has the potential to amplify existing socioeconomic disparities, civil liberties concerns, and ethics issues due to AI systems being developed using data that may reflect preexisting biases or social inequities. Additionally, there are increasing privacy risk concerns with the data collected by AI technologies and how the

Department uses and protects that data in its operations, investigations, prosecutions, and other activities. The OIG's oversight must ensure that the Department properly assesses and manages its use of this powerful and transformative technology. Without such assurances, the Department's use of AI technologies will be subject to abuse and could result in outcomes that stand counter to the mission of the Department and significantly damage public trust.

To keep pace with the evolving technological landscape, the OIG needs to recruit and retain personnel with both the functional and technical expertise to understand the applications and challenges that come when adopting emerging technologies, like AI, but have the skills and abilities to perform comprehensive oversight of the systems and the data involved. With this enhancement, the OIG would look to hire and contract for expertise in IT and cyber exploitation, as well as procure tools and applications to identify vulnerabilities. The additional staff will give the OIG the ability to adequately oversee the Department's use of AI and other emerging technologies to ensure these systems and programs are adding value, efficiency, and functioning as intended, while maintaining the imperative mission of upholding the rule of law, keeping the American people safe, and protecting civil rights. This increase in resources will ensure that the OIG can continue to provide Congress and the taxpayers with crucial and independent assessments of the DOJ's strategy and ethics principles in deploying this technology, as well as hold the Department accountable for the data gathered and used within such initiatives.

3. Current State and Impact on Performance

As evidenced by recent cyberattacks, there is little question that the Department continues to face ongoing and immediate IT security risks and, as a result, the Department's IT-related activities and costs continue to escalate to maintain its readiness to defend its critical national security and law enforcement missions against these attacks. Each year the OIG undertakes a significant work planning process that includes a robust risk assessment of programs and operations throughout the Department of Justice, and each year IT security and oversight of emerging technologies are identified as some of the highest-risk areas requiring vigorous OIG oversight. To date, the OIG has struggled to keep pace in this dynamic and rapidly evolving area due to limited resources, the increasing sophistication required to conduct such oversight, and persistent issue of competing priorities. If the requested funding is received, the OIG will be in a better position to dedicate resources with the required expertise in the relevant topics keep pace with the Department's growing use of technology throughout its operations and the sophistication of the IT industry. This enhancement will expand the OIG's ability to provide oversight in this area of increasing vulnerability and importance in view of the Department's expanding IT portfolio, the need to protect its networks, and the inevitable adoption by the Department of new technologies. Most importantly, these resources, if received, would allow the OIG to continue to expand upon the impactful work which the Department of Justice, Congress, and the American people have come to expect from the DOJ OIG.

Funding
Establish OIG's IT Security & Emerging Technology Oversight Unit
(Dollars in Thousands)

1. Base Funding

<i>FY 2023 Enacted</i>				<i>FY 2024 Continuing Resolution</i>				<i>FY 2025 Current Services</i>			
Pos	Agt/Atty	FTE	Amount (\$000)	Pos	Agt/Atty	FTE	Amount (\$000)	Pos	Agt/Atty	FTE	Amount (\$000)
0	0	0	\$0.00	0	0	0	\$0.00	0	0	0	\$0.00

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2025 Request (\$000)	Positions Requested	Full Year Modular Cost per Position (\$000)	Annualizations (\$000)			
				2 nd Year	3 rd Year	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Info Technology Mgmt (2210)	\$963.2	4	\$963.2	\$958.7	\$1,003.8	-\$4.6	\$45.10
Total Personnel	\$963.2	4	\$963.2	\$958.7	\$1,003.8	-\$4.6	\$45.10

3. Non-Personnel Increase

Non-Personnel Item	FY 2025 Request (\$000)	Unit Cost (\$000)	Quantity	Annualizations (\$000)	
				FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Contractor Services	\$550.0	\$275.0	2	\$5.5	\$5.6
Total Non-Personnel	\$550.0	\$275.0	2	\$5.5	\$5.6

4. Total Request for this Item

Category	Positions			Amount Requested (\$000)			Annualizations (\$000)	
	Count	Agt/Atty	FTE	Personnel	Non-Personnel	Total	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Current Services	0	0	0	0	0	0	N/A	N/A

Increases	4	0	4	\$963.2	\$550.0	\$1,513.0	\$0.9	\$50.7
Grand Total	4	0	4	\$963.2	\$550.0	\$1,513.0	\$0.9	\$50.7

5. Affected Crosscuts – Cybersecurity

Item Name: Cybersecurity and Information Technology Division Enhancement				
Strategic Goal(s) & Objective(s):	Strategic Goal 1: Uphold the Rule of Law Objective 1.1: Protect Our Democratic Institutions Objective 1.2: Promote Good Government Strategic Goal 2: Keep Our Country Safe Objective 2.4: Enhance Cybersecurity and Fight Cybercrime			
Organizational Program:	OIG			
Program Increase:	Positions 4	Agt/Atty 0/0	FTE 4	Dollars \$865,000
	Equipment/software/services:		Dollars \$1,020,000	
Total Request of Increase:	\$1,885,000			

1. Description of Item

In an effort for the OIG to meet the DOJ’s strategic goals and objectives of upholding the rule of law and keeping our country safe, the OIG requires a program enhancement of **\$1,885,000** and four positions to continue to modernize its information technology (IT) and enhance its internal cybersecurity posture to ensure that it can most effectively perform its important mission. The program enhancement focuses on three crucial areas: (1) enhancing the OIG’s cybersecurity posture, (2) modernizing the OIG’s business processes through the deployment of modern tools and automated applications, and (3) deployment of a classified case management system.

2. Justification

As part of our continual assessment of internal processes and practices to maximize the efficiency and economy of operations, the OIG requests the specific program enhancements described below to support its continually ongoing IT modernization initiative and achieve its mission to promote integrity, efficiency, and accountability within the DOJ.

(1) Enhance Cybersecurity and Combat Cybercrime –\$1.51M

The global cybersecurity landscape continues to see increased threats as organizations progress their digital transformation and cybercriminals continue to take advantage of misaligned networks. Check Point Research reported a 38 percent increase in global cyber-attacks in CY 2022. According to the GAO, the federal infrastructure is under increasing threats by malicious actors and constant attacks by nation-states. In FY 2021, Federal agencies reported 32,511 information security incidents. As a result, the OIG has remained vigilant in protecting system confidentiality, integrity, availability, and sensitive data, including personal identifiable information (PII). Maintaining this level of protection is imperative to preventing and responding to cyberattacks, even as the OIG sees its mission expand across unclassified, secret,

and top-secret enclaves. The growing number of cyber-related threats necessitates a unified approach to cybersecurity.

To adequately strategize and be proactive in addressing the increasing number of cyber-related threats while sustaining continuous oversight, protection, and monitoring of the OIG infrastructure, critical assets, and data, the OIG requests additional IT resources: IT Cyber Security Specialist, IT Helpdesk Specialist, Cloud Engineer, Software Developer, IT Project Manager, and eDiscovery Specialist. As the OIG endeavors to maintain a robust security posture, it requires the requested human capital resources to work together to achieve this goal. The IT Cyber Security Specialist ensures the organization continues to meet ever-growing cyber security standards. However, to save time and money on re-engineering efforts and ensure security is incorporated at the beginning of the process, other resources are also critical to protecting the OIG environment. The cloud engineer will ensure the infrastructure is configured and architected to meet defined cybersecurity standards. Currently, the IT Division only has one IT Software Developer, and adding another resource will fortify our cybersecurity infrastructure by minimizing vulnerabilities in software applications while ensuring new and core legacy applications are architected and developed to meet cyber standards and regulatory compliance. Moreover, with the increasing scope of work for the eDiscovery program, the eDiscovery specialist will further support the protection against external threats towards eDiscovery services by ensuring servers are adequately patched and vulnerabilities are remediated. In addition, the Helpdesk team serves as the first line of defense in identifying, coordinating, and remediating cyber-related incidents. Lastly, given the expansion of the OIG mission, the number of IT services and applications has increased. The IT Project Manager (PM) plays a vital role in overseeing the implementation of cybersecurity initiatives. The PM ensures that services and products purchased meet the cyber security supply chain requirements and Section 508 compliance by effectively managing resources, collaborating with internal and external stakeholders, and aligning project goals with the organization's cybersecurity strategy. A dedicated IT Project Manager can ensure cybersecurity projects have adequate coordination, direction, and oversight, while minimizing delays in implementing critical security enhancements, increased resource inefficiencies, and potential misalignment with industry best practices.

The DOJ OIG's IT division surveyed eight OIGs of similar size to determine the IT staff to employee ratio based on IT services provided to the enterprise. From the responses received, it is worth noting that OIGs of similar size had an average of one IT personnel for every 14 employees, while the DOJ OIG's ratio is one IT personnel for every 21 employees. Therefore, the additional resources will allow the IT Division to more effectively support the OIG workforce, and thereby strengthen our cybersecurity posture to bring us closer in alignment with other OIGs.

(2) Modernizing OIG Processes – \$210K

IT, facility, and division-level projects have increased significantly within the last year. As the complexity and number of organizational projects continue to grow, transparency and cross-collaboration amongst the divisions are crucial for project success. Currently, the OIG does not have a centralized project management platform to provide a 360-degree collaborative view of all projects and collaborative efforts. The program offices manage projects independently, relying heavily on fragmented manual processes, spreadsheets, and disparate project and program management applications. Utilizing these assortments of tools makes gathering project information, generating reports, and communicating project status inconsistent, time-consuming,

and error prone. Identifying resource availability, conflicts, and bottlenecks across competing projects and priorities becomes challenging. This can lead to suboptimal utilization of resources, delays in project delivery, and increased project costs. An integrated, scalable, centralized platform will satisfy the immediate need to standardize project management practices and methodologies, streamline processes, improve transparency and governance, optimize resource allocation, align projects with strategic goals and objectives, and enhance decision-making capabilities, ultimately leading to project success. Additionally, the OIG seeks to modernize its electronic fax (eFax) capabilities as part of its transition from a traditional VoIP platform to an integrated solution. This systems enhancement will provide the OIG with an efficient, secure, scalable platform that supports mobile, on-the-go capabilities.

(3) Classified Case Management System – \$170K

As the Investigations Division's (INV) classified work continues to grow, there is an immediate need to provide tools to improve management and tracking of this critically important work. Currently, INV does not have a classified case management system to record and process incoming classified complaints and manage classified criminal and administrative investigations. Due to this limitation, INV staff are required to print and maintain paper files for all classified work that does not allow staff from other offices to be able to review those files when necessary. Reproducing the OIG's existing unclassified case management system application into the classified environment would allow our field offices across the country to have a central repository for our classified work, improve the tracking of those complaints and investigations, and significantly improve the accessibility to our staff to work on these important matters. These improvements would enhance the OIG's management of its classified investigations portfolio, likely resulting in more timely completion of work, as well as enabling identification of potentially overlapping or conflicting investigations matters, thereby benefiting overall productivity.

3. Current State and Impact on Performance

Without the program enhancements listed above, the OIG will be limited in its ability to combat the rising cyber-related threats and stay abreast of emerging technologies, business processes, and industry best practices. The OIG will continue to provide and maintain legacy services and cannot comply with the White House Executive Order 14028, "Improving the Nation's Cybersecurity".

Funding
Cybersecurity and Information Technology Division Enhancement
(Dollars in Thousands)

1. Base Funding

<i>FY 2023 Enacted</i>				<i>FY 2024 Continuing Resolution</i>				<i>FY 2025 Current Services</i>			
Pos	Agt/Atty	FTE	Amount (\$000)	Pos	Agt/Atty	FTE	Amount (\$000)	Pos	Agt/Atty	FTE	Amount (\$000)
28	0	28	\$17,770.2	28	0	28	\$19,560.9	28	0	28	\$20,017.0

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2025 Request (\$000)	Positions Requested	Full Year Modular Cost per Position (\$000)	Annualizations (\$000)			
				2 nd Year	3 rd Year	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Info Technology Mgmt (2210)	\$865.0	4	\$865.0	\$834.2	\$874.9	-\$30.8	\$40.7
Total Personnel	\$865.0	4	\$865.0	\$834.2	\$874.9	-\$30.8	\$40.7

3. Non-Personnel Increase

Non-Personnel Item	FY 2025 Request (\$000)	Unit Cost (\$000)	Quantity	Annualizations (\$000)	
				FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Contractor Services	\$640.0	\$640.0	2	\$0.0	\$0.0
Project Tool	\$210.0	\$210.0	1	-\$140.0	\$6.0
Case Management System	\$170.0	\$170.0	1	\$0.0	\$0.0
Total Non-Personnel	\$1,020.0	\$275.0	2	\$880.0	\$6.0

4. Total Request for this Item

Category	Positions			Amount Requested (\$000)			Annualizations (\$000)	
	Count	Agt/Atty	FTE	Personnel	Non-Personnel	Total	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Current Services	28	0	28	\$7,664.0	\$12,683.0	\$20,017.0	N/A	N/A
Increases	4	0	4	\$865.0	\$1,020.0	\$1,885.0	\$228.2	\$287.2
Grand Total	32	0	32	\$8,529.0	\$13,703.0	\$22,232.0	\$228.2	\$287.2

5. Affected Crosscuts – Cybersecurity

Item Name: Prison Inspections Program Enhancement				
Strategic Goal(s) & Objective(s):	Strategic Goal 1: Uphold the Rule of Law Objective 1.1: Protect Our Democratic Institutions Objective 1.2: Promote Good Government Strategic Goal 2: Keep Our Country Safe Objective 2.1: Protect National Security Strategic Goal 5: Administer Just Court and Correctional Systems. Objective 5.2: Maintain a Safe and Humane Prison System			
Organizational Program:	OIG			
Program Increase:	Positions 8	Agt/Atty 0/0	FTE 8	Dollars \$1,569,600
	Equipment/software/services:		Dollars \$0	
Total Request of Increase:	\$1,569,600			

1. Description of Item

As part of the OIG’s ongoing efforts to provide robust oversight of the BOP, the Department requests a program increase of **\$1,569,600** and eight positions to enhance its efforts to assess and help the BOP improve the conditions of confinement in federal prisons. Specifically, Evaluation & Inspections Division (E&I) would like to expand its capacity to conduct unannounced, routine inspections of the 122 nationwide BOP prisons. E&I contains much of the OIG’s subject matter expertise relating to the conditions of confinement in federal prisons, having decades of experience evaluating the BOP’s programs, policies, and operations.

The additional funding will allow E&I to hire eight additional program analysts, which will increase its capacity to inspect federal prisons from two inspections per year to six inspections per year. These additional analysts will allow the division to inspect 5 percent (six of 122) prisons each year. As detailed below, these resources will enable the OIG to enhance its BOP oversight and continue to shed light on the conditions of confinement in federal prisons and by collecting data that will help stakeholders better understand the longstanding systemic challenges facing the BOP and their impact on BOP inmates and staff.

2. Justification

Federal offenders have a constitutional right to humane conditions of confinement. Specifically, in its prohibition of “cruel and unusual punishments,” the Eighth Amendment imposes a duty upon prison officials (1) to provide humane conditions of confinement; (2) to ensure that inmates receive adequate food, clothing, shelter, and medical care; and (3) to “take reasonable measures

to guarantee the safety of the inmates.” *Farmer v. Brennan*, 511 U.S. 825, 832 (1994) (citing *Hudson v. Palmer*, 468 U.S. 517, 526-27 (1984)). Accordingly, the Department has identified maintaining a safe and humane federal correctional system as a key priority in its FY 2022-2026 Strategic Plan, and the BOP has long identified fostering “a humane and secure environment” as a core part of its mission. However, in recent years, many of the OIG’s stakeholders, including Congress and non-governmental organizations, have expressed concerns about the BOP’s ability to provide humane conditions of confinement to federal inmates, citing such incidents as the high-profile deaths of inmates Whitey Bulger and Jeffrey Epstein, the widespread sexual abuse of inmates at FCI Dublin, and allegations of inmate mistreatment at USP Thomson. Moreover, in April 2023, the U.S. Government Accountability Office (GAO) added [Strengthening the Management of the Federal Prison System](#) to its high-risk list, citing multiple longstanding issues that “present a serious threat to inmate and staff safety.” Absent sufficient independent, onsite oversight of the conditions of confinement in federal prisons, such as that provided by the OIG’s routine prison inspection program, it will be difficult to determine whether the Department is achieving these goals or whether stakeholder concerns are addressed.¹

The OIG has long raised concerns about the conditions of confinement in federal prisons, having consistently listed the management of federal prisons as one of the Department’s top management and performance challenges for over 20 years.² E&I, in particular, has issued a number of reports highlighting concerns relating to the conditions in which federal offenders are confined, such as the BOP’s management of female inmates; its use of restrictive housing for inmates with mental illness; and its monitoring of contract prisons. In addition, OIG reporting resulting from E&I reviews has highlighted significant issues with system-wide deficiencies in video surveillance cameras, employee screening for contraband, mental health treatment for inmates, First Step Act compliance, and the compassionate release program, among other concerns. More recently, E&I has increased its efforts to provide greater transparency into the conditions of confinement in BOP institutions by conducting multiple surveys of BOP inmates and staff and by establishing a routine inspection program wherein E&I analysts conduct unannounced inspections of BOP facilities. The results of the OIG’s inspection program, as evidenced by its initial report of the inspection of FCI Waseca, have been eye-opening.

However, while the OIG has provided robust oversight of the BOP for decades in the form of audits, evaluations, and investigations, it continues to lack the resources for a robust routine prison inspection program. For example, between 1996 and 2019, E&I did not conduct any prison inspections, in part because of its limited staff and resources. In 2019, the Deputy Attorney General requested that the OIG inspect the conditions of confinement at the Metropolitan Detention Center in Brooklyn, New York following a power outage during the coldest months of the year. To comply with this request, E&I was forced to put two evaluations on hold. Similarly, in April 2020, the Attorney General requested that the OIG conduct a series of inspections to assess the BOP’s response to the COVID-19 pandemic. Recognizing the importance of providing oversight in this area, E&I put nine ongoing evaluations on hold (90 percent of its workload), redirected the efforts of 24 E&I program analysts, and acquired 35

¹ Although the BOP has its own internal audit function, a May 2023 OIG report on BOP strategies to identify, communicate, and remedy operational issues identified weaknesses in the BOP’s internal audit function.

² See, for example, the OIG’s [FY 2022 Top Management and Performance Challenges](#) report. In the report, the OIG highlighted a myriad of long-standing challenges for the BOP that impact the conditions of confinement, including insufficient staffing, an inadequate security camera system, impediments to ensuring inmate and staff safety, contraband introductions, and the physical deterioration of its institutions.

detailed employees from other OIG divisions to conduct 16 remote inspections of facilities housing BOP inmates, including federal correctional institutions, contract institutions, and Residential Reentry Centers (i.e., “halfway houses”).

In FY 2023, the OIG received funding for five additional analysts (bringing E&I from 35 to 40 authorized employees) for the creation of its BOP Interdisciplinary Oversight Team. The team combines OIG inspectors, auditors, and investigators who can leverage their broad experience, resources, and data to collaborate on the most pressing BOP enterprise-wide challenges. With those five analysts (four analysts dedicated to conducting prison inspections and one program manager tasked with managing E&I’s extensive portfolio of BOP oversight projects) and the temporary reassignment of 15 employees from other projects, E&I was able to build the infrastructure needed to support the initial launch of its routine inspection program. That work included creating a risk assessment tool to inform the selection of inspection sites, developing a standardized methodology for targeted information collection, and integrating outside prison medical experts in the inspections. In February 2023, E&I completed its first-ever unannounced routine prison inspection at FCI Waseca and issued an [impactful report](#) in May 2023. In late May, E&I initiated its second unannounced inspection at FCI Tallahassee and is on track to initiate a third inspection in FY 2023. However, E&I will not be able to maintain this rate of initiation of new inspections without the requested eight analysts, or to grow its inspection program to provide adequate coverage of the BOP’s 122 institutions. With only four analysts dedicated to BOP inspections, E&I can only conduct one or two inspections a year, depending on the complexity of the institutions inspected. The current limitation on the number of analysts devoted to inspections is necessary to enable E&I to continue its other important oversight work of BOP and other Department programs. For example, E&I has recently concluded an evaluation of gender equity within the Federal Bureau of Investigation’s training process and assessed sexual misconduct by BOP inmates directed at staff.

The eight requested analysts would allow E&I to routinely inspect five percent of all BOP institutions (six of 122) of varying facility types, security levels, and geographic regions each year, with a focus on institutions that have the greatest risk. The Division’s routine prison inspections complement its existing evaluations of systemic issues by providing timely, risk-based oversight of BOP institutions and identifying areas needing immediate attention. Inspection reports are effective in communicating problem areas quickly and succinctly as they are short in length, narrowly scoped, and contain photographs depicting near real-time conditions of confinement. For example, immediately following publication of our FCI Waseca inspection report which identified and included photographs of unsafe conditions in some inmate housing areas, the BOP relocated affected inmates. As OIG inspection teams interview staff and inmates, photograph physical conditions, and review documentation during unannounced inspections, the resulting reports provide for all stakeholders a well-rounded, independent snapshot of the conditions of confinement at an institution. In addition, the inspections would provide greater insight into the impact of longstanding BOP management issues, including those identified by the GAO and other stakeholders, both at the institution level and systemically.

The Department, the BOP Director, and several members of Congress have been supportive of the OIG’s establishment of its routine inspection program, recognizing that independent, thorough OIG inspections provide OIG stakeholders, including BOP leadership, reliable information on the conditions of confinement in federal prisons that would not otherwise be available. Accordingly, E&I has had increasing demands for additional prison inspections that it cannot satisfy with its current staffing level. Enhancing E&I’s inspection capacity will allow for

greater transparency into federal prison conditions and will also allow E&I to continuously identify, assess, and track significant risks in BOP programs and operations, thereby helping the OIG determine and prioritize oversight priorities and the most effective use of OIG resources.

3. Current State and Impact on Performance

With its current staffing levels, E&I cannot conduct enough prison inspections to provide true insight into the conditions of confinement in federal prisons. At present, the BOP has 122 prisons, while E&I only has four analysts dedicated to inspections of those institutions. Without the requested enhancement, E&I will only be able to inspect one or two prisons a year, which will make it impossible to fully implement its risk-based selection tool. Therefore, E&I will not be able to inspect the institutions with the highest risk of noncompliance with BOP and ACA guidance on conditions of confinement, nor identify areas needing immediate attention from BOP leadership.

Funding
Prison Inspections Program Enhancement
(Dollars in Thousands)

1. Base Funding

<i>FY 2023 Enacted</i>				<i>FY 2024 Continuing Resolution</i>				<i>FY 2025 Current Services</i>			
Pos	Agt/Atty	FTE	Amount (\$000)	Pos	Agt/Atty	FTE	Amount (\$000)	Pos	Agt/Atty	FTE	Amount (\$000)
40	0	40	\$7,449.3	40	0	40	\$7,836.7	40	0	40	\$8,228.5

2. Personnel Increase Cost Summary

Type of Position/Series	FY 2025 Request (\$000)	Positions Requested	Full Year Modular Cost per Position (\$000)	Annualizations (\$000)			
				2 nd Year	3 rd Year	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Clerical and Office Svcs (0300-0399)	\$1,569.6	8	\$1,569.6	\$1,537.8	\$1,612.3	-\$31.8	\$74.5
Total Personnel	\$1,569.6	8	\$1,569.6	\$1,537.8	\$1,612.3	-\$31.8	\$74.5

3. Total Request for this Item

Category	Positions			Amount Requested (\$000)			Annualizations (\$000)	
	Count	Agt/Atty	FTE	Personnel	Non-Personnel	Total	FY 2026 (net change from 2025)	FY 2027 (net change from 2026)
Current Services	40	0	40	\$8,225.5	0	\$8,225.5	N/A	N/A
Increases	8	0	8	\$1,569.6	0	\$1,569.6	-\$31.8	\$74.5
Grand Total	48	48	48	\$9,798.1	0	\$9,798.1	-\$31.8	\$74.5

4. Affected Crosscuts – N/A

VII. Appendix

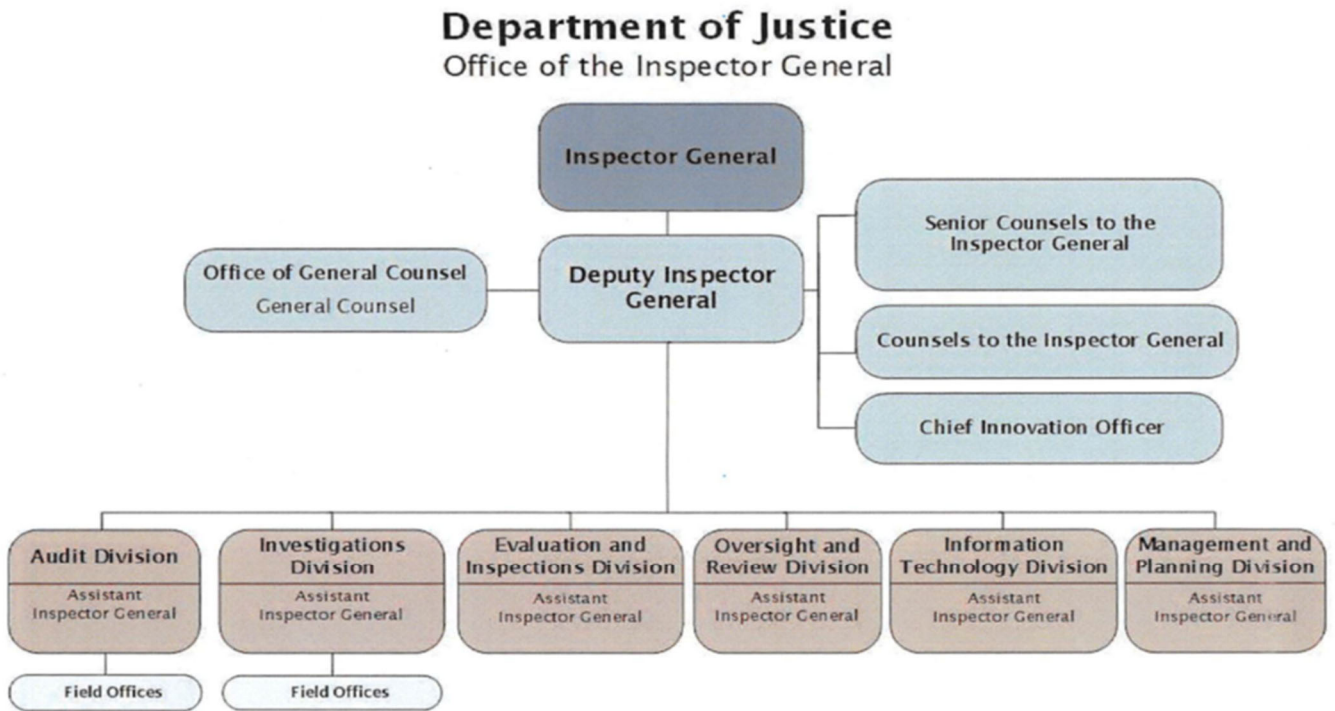
A. Statistical Highlights

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, 2023 – September 30, 2023	
Allegations Received by the Investigations Division	7,826
Investigations Opened	93
Investigations Closed	125
Arrests	42
Indictments/Information	40
Convictions/Pleas	44
Administrative Actions	84
Monetary Recoveries	\$ 6,036,992
Audit Reports Issued	37
Questioned Costs	\$ 1,204,372
Recommendations for Management Improvements	151
<i>Single Audit Act</i> Reports Issued	12
Recommendations for Management Improvements	26

VIII. Exhibits

A. Organizational Chart



Approved by:  Date: 2/11/19
Michael E. Horowitz
Inspector General

B. 1. Summary of Requirements

Summary of Requirements

Office of the Inspector General

Salaries and Expenses

(Dollars in Thousands)

	FY 2025 Request		
	Positions	Estimate FTE	Amount
2023 Enacted 1/	560	516	149,000
Total 2023 Enacted	560	516	149,000
2024 Continuing Resolution	560	535	149,000
FY 2024 Annualized Continuing Resolution	-14	-14	0
Total 2024 Continuing Resolution	546	521	149,000
Technical Adjustments			
Additional Amount for 2024 Pay Raise	0	0	3,000
Non-Recrural - Oversight and Auditing - From CVF	0	0	-10,000
Oversight and Auditing - From CVF	0	0	5,000
Total Technical Adjustments	0	0	-2,000
Base Adjustments			
Transfers:			
Transfers - Oversight and Auditing - From CVF	0	0	5,000
Pay and Benefits	0	0	5,552
Domestic Rent and Facilities	0	0	346
Other Adjustments	0	0	150
Total Base Adjustments	0	0	11,048
Total Technical and Base Adjustments	0	0	9,048
2025 Current Services	546	521	158,048
Program Changes			
Increases:			
Civil Rights Violations, Cybercrime, and Fraud Investigations	8	8	1,889
Cybersecurity and Technology Enhancement	0	0	4,865
Cybersecurity and Information Technology Division Enhancement	4	4	1,885
National Security Oversight	8	8	1,820
Prison Inspection Program Enhancement	8	8	1,570
Security and Emerging Technology Enhancement	4	4	1,513
Subtotal, Increases	32	32	13,542
Total Program Changes	32	32	13,542
2025 Total Request	578	553	171,590
2024 - 2025 Total Change	32	32	22,590

^{1/} FY 2023 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 2023 Enacted			FY 2024 Continuing Resolution			FY 2024 Annualized Continuing Resolutuion			FY 2025 Technical and Base Adjustments			FY 2025 Current Services		
	Position s	Actual FTE	Amount	Positions	Est. FTE	Amount	Position s	Est. FTE	Amount	Position s	Est. FTE	Amount	Position s	Est. FTE	Amount
OIG Audits, Inspections, Investigations, and Reviews	560	535	149,000	560	535	149,000	-14	-14	0	0	0	9,048	546	521	158,048
Total Direct	560	535	149,000	560	535	149,000	-14	-14	0	0	0	9,048	546	521	158,048
Balance Rescission			0			0			0			0			0
Total Direct with Rescission			149,000			149,000			0			9,048			158,048
Reimbursable FTE		20			20			0		2				22	
Total Direct and Reimb. FTE		555			555			-14		2				543	
Other FTE:															
LEAP		0			0			0		0				0	
Overtime		0			0			0		0				0	
Grand Total, FTE		555			555			-14		2				543	

Program Activity	2025 Increases			2025 Offsets			2025 Request		
	Position s	Est. FTE	Amount	Positions	Est. FTE	Amount	Position s	Est. FTE	Amount
OIG Audits, Inspections, Investigations, and Reviews	32	32	13,542	0	0	0	578	553	171,590
Total Direct	32	32	13,542	0	0	0	578	553	171,590
Balance Rescission			0			0			0
Total Direct with Rescission			13,542			0			171,590
Reimbursable FTE		0			0			22	
Total Direct and Reimb. FTE		32			0			575	
Other FTE:									
LEAP		0			0			0	
Overtime		0			0			0	
Grand Total, FTE		32			0			575	

C. Summary of Requirements by Decision Unit

FY 2025 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
Civil Rights Violations, Cybercrime, and Fraud Investigations		8	8	8	1,889	8	8	8	1,889
Cybersecurity and Technology Enhancement		0	0	0	4,865	0	0	0	4,865
Cybersecurity and Information Technology Division Enhancement		4	0	4	1,885	4	0	4	1,885
National Security Oversight		8	1	8	1,820	8	1	8	1,820
Prison Inspection Program Enhancement		8	0	8	1,570	8	0	8	1,570
Security and Emerging Technology Enhancement		4	0	4	1,513	4	0	4	1,513
Total Program Increases		32	9	32	13,542	32	9	32	13,542

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 2023 Enacted		FY 2024 Continuing Resolution		FY 2025 Current Services		FY 2025 Increases		FY 2025 Offsets		FY 2025 Total Request	
	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	Direct & Reimb FTE	Direct Amount
Goal 1 Uphold the Rule of Law												
1.1 Protect Our Democratic Institutions.	536	149,000	541	149,000	543	158,048	32	13,542	0	0	575	171,590
Subtotal, Goal 1	536	149,000	541	149,000	543	158,048	32	13,542	0	0	575	171,590
TOTAL	536	149,000	541	149,000	543	158,048	32	13,542	0	0	575	171,590

E. Justification for Technical and Base Adjustments

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

	Positions	Estimate FTE	Amount
Technical Adjustments			
1 Additional Amount for 2024 Pay Raise	0	0	3,000
2 Non-Recrural - Oversight and Auditing - From CVF Non-recrural of FY 2024 \$10M Direct transfer from CVF.	0	0	-10,000
3 Oversight and Auditing - From CVF In 2025, \$5M from CVF will be included in Direct funding	0	0	5,000
Subtotal, Technical Adjustments	0	0	-2,000
Transfers			
1 Transfers - Oversight and Auditing - From CVF In 2025, \$5M Direct transfer from CVF.	0	0	5,000
Subtotal, Transfers	0	0	5,000
Pay and Benefits			
1 <u>2025 Pay Raise - 2%</u> This request provides for a proposed 2 percent pay raise to be effective January of 2025. The amount requested, \$1,774,000 represents the pay amounts for 3/4 of the fiscal year plus appropriate benefits (\$1,135,000 for pay and \$639,000 for benefits).	0	0	1,774
2 <u>Annualization of 2023 Approved Positions</u> Personnel: This provides for the third-year annualization of 21 new positions appropriated in 2023. 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 2023 increases, this request includes an increase of \$1,911,000 for full-year payroll costs associated with these additional positions.	0	0	1,911
3 <u>Annualization of 2024 Pay Raise</u> This pay annualization represents first quarter amounts (October through December) of the 2024 pay increase of 5.2%. The amount requested, \$1,394,000, represents the pay amounts for 1/4 of the fiscal year plus appropriate benefits (\$892,160 for pay and \$501,840 for benefits.)	0	0	1,394
4 <u>Employees Compensation Fund</u> Employees Compensation Fund	0	0	7
5 <u>Health Insurance</u> Effective January 2024, the component's contribution to Federal employees' health insurance increases by 7.4% percent. Applied against the 2024 estimate of \$6,278,000, the additional amount required is \$466,000.	0	0	466
Subtotal, Pay and Benefits	0	0	5,552
Domestic Rent and Facilities			
1 <u>GSA Rent</u> GSA will continue to charge rental rates that approximate those charged to commercial tenants for equivalent space and related services. The requested increase of \$220,000 is required to meet our commitment to GSA. The costs associated with GSA rent were derived through the use of an automated system, which uses the latest inventory data, including rate increases to be effective FY 2025 for each building currently occupied by Department of Justice components, as well as the costs of new space to be	0	0	334
2 <u>Guard Service</u> This includes Department of Homeland Security (DHS) Federal Protective Service charges, Justice Protective Service charges and other security services across the country. The requested increase of \$12,000 is required to meet these commitments.	0	0	12
Subtotal, Domestic Rent and Facilities	0	0	346
Other Adjustments			
1 <u>Council of the IG on Integrity and Efficiency Contribution</u> Council of the IG on Integrity and Efficiency Contribution - Under authority of the IG Act of 1978 (as amended by the IG Reform Act of 2008) Section 11.c.3.A.	0	0	150
Subtotal, Other Adjustments	0	0	150
TOTAL DIRECT TECHNICAL and BASE ADJUSTMENTS	0	0	9,048
ATB Reimbursable FTE Changes			
1 ATB Reimbursable Position/FTE Adjustment	0	2	0
Subtotal, ATB Reimbursable FTE Changes	0	2	0

F. Crosswalk of 2023 Availability

Crosswalk of 2023 Availability

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

Program Activity	FY 2023 Enacted			Reprogramming/Transfers			Carryover	Recoveries /Refunds	FY 2023 Availability		
	Position s	Est. FTE	Amount	Position s	Est. FTE	Amount	Amount	Amount	Position s	Est. FTE	Amount
OIG Audits, Inspections, Investigations, and Reviews	560	535	139,000	0	0	10,800	22,860	1,247	560	535	173,907
Total Direct	560	535	139,000	0	0	10,800	22,860	1,247	560	535	173,907
Balance Rescission			0			0	0	0			0
Total Direct with Rescission			139,000			10,800	22,860	1,247			173,907
Reimbursable FTE		20			0					20	
Total Direct and Reimb. FTE		555			0					555	
Other FTE:											
LEAP FTE		0			0					0	
Overtime		0			0					0	
Grand Total, FTE		555			0					555	

Reprogramming/Transfers:

\$10.0 million transfer from CVF per PL 117-103.

\$800,000 transfer from FY 2022 annual fund to FY 2022/2023 multiyear fund.

Carryover:

\$19.2 million in CVF transfer carryover.

\$2.8 million in FY 2022/2023 multiyear carryover.

\$811,000 in FY 2022/2023 HCFAC carryover.

Recoveries/Refunds:

\$158,000 recovery of prior-year unpaid obligations.

\$1.1 million in HCFAC collections in FY 2023/2024 multiyear fund.

G. Crosswalk of FY 2024 Availability

Crosswalk of 2024 Availability
Office of the Inspector General
Salaries and Expenses
(Dollars in Thousands)

Program Activity	FY 2024 Continuing Resolution			FY 2024 Annualized Continuing Resolutuion			Reprogramming/Transfers			Carryover	Recoveries /Refunds	FY 2024 Availability			
	Position s	Est. FTE	Amount	Position s	Est. FTE	Amount	Positions	Est. FTE	Amount			Amount	Amount	Position s	Est. FTE
OIG Audits, Inspections, Investigations, and Reviews	560	535	149,000	-14	-14	0	0	0	10,000	21,621		200	546	521	180,821
Total Direct	560	535	149,000	-14	-14	0	0	0	10,000	21,621		200	546	521	180,821
Balance Rescission			0			0			0	0		0			0
Total Direct with Rescission			149,000			0			10,000	21,621		200			180,821
Reimbursable FTE		20			0			0							20
Total Direct and Reimb. FTE		555			-14			0							541
Other FTE:															
LEAP FTE		0			0			0							0
Overtime		0			0			0							0
Grand Total, FTE		555			-14			0							541

Reprogramming/Transfers:

\$10.0 million transfer from the CVF.

Carryover:

\$16.8 million in CVF transfer carryover.

\$4.0 million in FY 2023/2024 multiyear carryover.

\$830,000 in FY 2023/2024 HCFAC carryover.

Recoveries/Refunds:

\$200,000 in estimated HCFAC collections in FY 2024/2025 multiyear fund.

H.R. Summary of Reimbursable Resources

Summary of Reimbursable Resources

Office of the Inspector General

Salaries and Expenses

(Dollars in Thousands)

Collections by Source	2023 Actual			2024 Estimate			2025 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	1,372	0	0	0	0	0	0	0	0	0
Council of the IGs on Integrity and Efficiency	1	1	420	1	1	405	1	1	413	0	0	8
Bureau of Alcohol, Tobacco, Firearms and Explosives	0	0	100	0	0	0	0	0	50	0	0	50
Working Capital Fund	7	6	2,953	7	6	3,093	7	6	3,155	0	0	62
Federal Bureau of Investigation	2	2	1,998	0	0	0	0	0	0	0	0	0
Federal Prison Industries	2	2	1,231	0	0	200	0	0	0	0	0	-200
Offices, Boards, and Divisions	8	7	7,525	14	13	12,223	14	15	12,471	0	2	248
Budgetary Resources	22	20	15,599	22	20	15,921	22	22	16,089	0	2	168

Obligations by Program Activity	2023 Actual			2024 Estimate			2025 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	22	20	15,599	22	20	15,921	22	22	16,089	0	2	168
Budgetary Resources	22	20	15,599	22	20	15,921	22	22	16,089	0	2	168

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

Summary of Sub-Allotments and Direct Collections Resources

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

Sub-Allotments and Direct Collections	2023 Actual			2024 Estimate			2025 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										0	0	0

Obligations by Program Activity	2023 Actual			2024 Estimate			2025 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										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 2023 Enacted		FY 2024 Continuing Resolution		FY 2025 Request				
	Direct Pos.	Reimb. Pos.	Direct Pos.	Reimb. Pos.	ATBs	Program Increases	Program Offsets	Total Direct Pos.	Total Reimb. Pos.
Security Specialists (080)	4	0	4	0	0	0	0	4	0
Human Resources Management (0200-0260)	10	0	10	0	0	0	0	10	0
Clerical and Office Services (0300-0399)	158	4	152	4	-83	10	0	79	4
Accounting and Budget (500-599)	148	14	145	14	83	5	0	233	14
Attorneys (905)	50	0	49	0	0	1	0	50	0
Paralegal Specialist (0950)	2	0	2	0	0	0	0	2	0
Information & Arts (1000-1099)	4	0	4	0	0	0	0	4	0
Operations Research Analyst	1	0	1	0	0	0	0	1	0
Statistician (1530)	1	0	1	0	0	0	0	1	0
Inspection, Investigation, Enforcement Analyst(1801)	5	0	5	0	0	0	0	5	0
Misc. Inspectors/Investigative Assistants (1802)	6	0	6	0	0	0	0	6	0
Criminal Investigative Series (0082 & 1811)	146	0	142	0	0	8	0	150	0
Information Technology Mgmt (2210-2299)	25	4	25	4	0	8	0	33	4
Total	560	22	546	22	0	32	0	578	22
Headquarters Washington D.C.	237	22	230	22	0	16	0	246	22
US Fields	323	0	316	0	0	16	0	332	0
Foreign Field	0	0	0	0	0	0	0	0	0
Total	560	22	546	22	0	32	0	578	22

* Due to an OPM audit, OIG needed to reclassify 83 positions from the 0300-0399 series to the 0500-0599 series, assigning new positions descriptions, to comply with OPM requirements.

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	3	828	0	0	3	828
GS-14	7	913	0	0	7	913
GS-13	22	5,347	0	0	22	5,347
Ungraded	0	6,454	0	0	0	6,454
Total Positions and Annual Amount	32	13,542	0	0	32	13,542
Lapse (-)	0	-9,007	0	0	0	-9,007
11.5 - Other personnel compensation		0		0		0
Total FTEs and Personnel Compensation	32	4,535	0	0	32	4,535
12.1 - Civilian personnel benefits		2,552		0		2,552
25.3 - Other goods and services from federal sources		1,589		0		1,589
25.7 - Operations and Maintenance of Equipment		4,865		0		4,865
Total Program Change Requests	32	13,542	0	0	32	13,542

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 2023 Actual		FY 2024 Continuing Resolution		FY 2025 Request		Increase/Decrease	
	Act. FTE	Amount	Direct FTE	Amount	Direct FTE	Amount	Direct FTE	Amount
11.1 - Full-time permanent	516	72,900	521	69,949	553	82,013	32	12,064
11.3 - Other than full-time permanent	0	2,766	0	2,766	0	2,766	0	0
11.5 - Other personnel compensation	0	4,867	0	4,867	0	4,867	0	0
<i>Overtime</i>	0	0	0	0	0	0	0	0
<i>Other Compensation</i>	0	0	0	0	0	0	0	0
11.8 - Special personal services payments	0	0	0	0	0	0	0	0
Total	516	80,533	521	77,582	553	89,646	32	12,064
Other Object Classes								
12.1 - Civilian personnel benefits		37,830		34,535		41,695	0	7,160
21.0 - Travel and transportation of persons		2,209		2,253		2,298	0	45
23.1 - Rental payments to GSA		11,917		11,696		12,042	0	346
23.2 - Rental payments to others		284		290		295	0	6
23.3 - Communications, utilities, and miscellaneous charges		1,705		1,739		1,774	0	35
24.0 - Printing and reproduction		0		37		37	0	1
25.1 - Advisory and assistance services		2,728		2,222		2,266	0	44
25.2 - Other services from non-federal sources		454		463		472	0	9
25.3 - Other goods and services from federal sources		5,127		8,334		15,071	0	6,737
25.4 - Operation and maintenance of facilities		1,293		1,319		1,345	0	26
25.7 - Operation and maintenance of equipment		2,714		3,988		8,937	0	4,950
26.0 - Supplies and materials		1,122		1,515		1,545	0	30
31.0 - Equipment		4,018		4,088		4,480	0	392
Total Obligations		151,934		150,060		181,905	0	31,845
Net of:								
Unobligated Balance, Start-of-Year		-22,860		-21,621		-22,227	0	-606
Transfers/Reprogramming		-10,800		-10,000		-5,000	0	5,000
Recoveries/Refunds		-1,247		-1,666		-1,666	0	0
Balance Rescission		0		0		0	0	0
Unobligated End-of-Year, Available		21,621		22,227		13,578	0	-8,649
Unobligated End-of-Year, Expiring		352		0		0	0	0
Total Direct Requirements		139,000		139,000		166,590		27,590
Reimbursable FTE								
Full-Time Permanent	20		20		22		2	0

Non-SES/SL/ST Salary	65,503	69,664	75,287
Non-SES/SL/ST Award (FY2023 = 2.5% of FY2022 Salary, FY2024 = 2.5% of FY2023 Salary, FY2025 = 2.5% of FY2024 estimated Salary)	1,638	1,742	1,882

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 \$171,590,000;

The requested amount includes \$666,360 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 \$1,292,000

The Inspector General of the Department of Justice certifies that the amount requested for training satisfies all OIG training needs of FY 2025.

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 \$171,590,000;

The requested amount includes \$666,360 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 \$1,292,000

The Inspector General of the Department of Justice certifies that the amount requested for training satisfies all OIG training needs of FY 2025.