U.S. Department of Justice
FY 2022 PERFORMANCE BUDGET

Office of the Inspector General

Congressional Justification

Contents

I. Overview (Office of the Inspector General)

A. Introduction

In Fiscal Year (FY) 2022, the President's budget request for the Department of Justice (DOJ) Office of the Inspector General (OIG) totals $137.2 million, which includes $10 million from the Crime Victims Fund (CVF) for oversight of CVF, 549 FTE (529 Direct and 20 Reimbursable), and 539 positions (146 agents and 35 attorneys) to investigate allegations of fraud, waste, abuse, and misconduct by DOJ employees, contractors, and grantees and to promote economy and efficiency in Department operations. Additionally, the OIG is requesting $4 million in annual carryover authority.

B. Background

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

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

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

C. OIG Organization

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

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

Investigations Division is responsible for investigating allegations of bribery, fraud, abuse, civil rights violations, and violations of other criminal laws and administrative procedures governing Department employees, contractors, and grantees. The Investigations Division has field offices in Chicago, Dallas, Denver, Los Angeles, Miami, New York, and Washington, D.C. The Fraud Detection Office and the Cyber Investigations Office are located in Washington, D.C. The Investigations Division has smaller area offices in Atlanta, Boston, Trenton, Detroit, El Paso, Houston, San Francisco, and Tucson. Investigations Headquarters in Washington, D.C., consists of the Immediate Office of the Assistant Inspector General for Investigations and the following branches: Operations, Operations II, Investigative Support, and Administrative Support.

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

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

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

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

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

D. Notable Highlights, Reviews, and Recent Accomplishments

1. Strengthening Public Confidence in Law Enforcement and Protecting Civil Liberties

One of the most pressing challenges facing the Department of Justice (DOJ or the Department), in the wake of nationwide protests following the deaths of George Floyd, Breonna Taylor, and Ahmaud Arbery, among other incidents, is how it can most effectively work to strengthen public confidence in law enforcement and protect individuals' civil liberties. This is not a new challenge for the Department. The OIG's 2015 Top Management and Performance Challenges (TMPC) report identified building trust and improving police-community relations as among the most pressing challenges for the Department after police killings of unarmed African Americans in Ferguson, Missouri, and Baltimore, Maryland.

Community trust and cooperation are essential to effective policing. In its dual roles as policy leader and law enforcer, the Department has numerous tools at its disposal to safeguard individual rights and promote constitutional policing practices at the state and local levels. As the nation's leading law enforcement agency, the Department must also ensure that its own law enforcement components, while fulfilling their critical law enforcement missions, adhere to constitutional and statutory constraints designed to protect individuals' civil rights, civil liberties, and privacy.

The Department Plays a Critical Role in Ensuring Public Confidence in Law Enforcement

Recent tragic confrontations between police and private citizens—and resulting protests and civil unrest—have brought to the fore a public concern that Black people receive disparate treatment at the hands of law enforcement. A 2019 Pew Research Center survey found that "majorities of both black and white Americans say blacks are treated less fairly than whites in dealing with police and by the criminal justice system as a whole" and that "black adults are about five times as likely as whites to say they've been unfairly stopped by police because of their race or ethnicity."[1]

The Attorney General has heard concerns that "African Americans often feel 'treated as suspects first and citizens second'" and remarked, "I think these concerns are legitimate." [2]In addressing the tension between enforcing the law and upholding the civil rights of all citizens, the Attorney General stated: "While the vast majority of police officers do their job bravely and righteously, it is undeniable that many African Americans lack confidence in the American criminal justice system. That must change. Our constitution mandates equal protection of the laws, and nothing less is acceptable. As the nation's leading federal law-enforcement agency, the Department of Justice will do its part."[3]

Presidential Commission on Law Enforcement and the Administration of Justice

---

[1] Pew Research Center, "10 Things we Know About Race and Policing in the U.S.," June 3, 2020 (accessed August 13, 2020).
[2] William P. Barr, Attorney General, "Opening Statement Before the House Judiciary Committee," July 28, 2020, www.justice.gov/opa/speech/opening-statement-attorney-general-william-p-barr-house-judiciary-committee (accessed September 14, 2020).

[3] William P. Barr, Attorney General, "Remarks on Mr. George Floyd and Civil Unrest," June 4, 2020, www.justice.gov/opa/speech/attorney-general-william-p-barr-s-remarks-mr-george-floyd-and-civil-unrest (accessed September 14, 2020).

In January 2020, the Department established the Presidential Commission on Law Enforcement and the Administration of Justice (the Commission), and in December 2020, a final report was released, and can be found here.

The thesis of the Commission's study is that the fundamental duty of law enforcement remains to protect people from harm. It accomplishes this duty directly through safeguarding victims from crime and indirectly through maintaining the rule of law. No segment of the criminal justice system—courts, prosecutors, prisons—has been as effective or successful at crime reduction as law enforcement. A robust police force remains essential for public safety and the legal order, and under these circumstances there must be more, not less, investment in law enforcement to protect and serve American communities.

In part due to its success addressing criminal problems, impractical expectations have arisen that law enforcement officers can cure all the criminal problems they police, which has resulted in an overworked, overburdened law enforcement with diminished resources, morale, and public confidence. The fact remains that crime is a complex social problem that requires a conglomerate of welfare programs and government systems to address, and thus requires the help of a greater social and governmental framework to reduce. With this understanding, law enforcement can return to its core mission and first duty—public safety. This is a demanding responsibility. While there are many ways for law enforcement to improve its capacity to address the salient criminal threats of our time, enhanced technology and crime data analysis hold extraordinary promise for the ability of law enforcement to fashion smart, efficient, and evidence-based strategies to police a 21st century world and preserve collective peace and security.

Criminal and Civil Enforcement Targeting Civil Rights Violations by Police

The Department's Civil Rights Division (CRT) has authority under 18 U.S.C. § 242 to prosecute individual law enforcement officers for willful civil rights violations. CRT also has authority, under 34 U.S.C. § 12601 (formerly 42 U.S.C. § 14141), to investigate police departments for patterns or practices of unconstitutional policing and to bring civil enforcement actions or seek other forms of relief where such pattern or practice is found. In June 2020, CRT took a positive step forward by launching a "Civil Rights Reporting Portal," which makes it easier for the public to report civil rights violations, including misconduct by law enforcement officers. Given recent events, however, there have been bipartisan calls for the Department to maximize use of its pattern-or-practice authority to establish accountability and public trust in law enforcement. The Department faces challenges in balancing its stated policy favoring local control and local accountability over nonfederal law enforcement agencies with the need to assure the public that the Department is using its available authorities to vindicate and prevent civil rights violations in policing at the state and local levels.

Leading by Example Through the Department's Law Enforcement Components

The Department's law enforcement components provide crucial assistance to state and local law enforcement agencies responding to civil unrest. The Department must ensure, however, that in doing so its law enforcement components respect the civil rights and civil liberties of peaceful protesters exercising their right to free expression. The Department's Annual Performance Plan for Fiscal Year 2021 identified defending the First Amendment right to free speech as one of the Department's top strategic objectives.

Body-worn Cameras and Law Enforcement Identification

Body-worn cameras (BWC) are one tool available to law enforcement to improve transparency and accountability and, thereby, build the trust of the communities they serve. According to OJP, since 2015, the Department's Bureau of Justice Assistance has provided more than $113 million to state, local, and tribal agencies through its Body-Worn Camera Policy and Implementation Program, with over $20 million provided in fiscal year (FY) 2019 alone. As a policy leader, the Department can set an example for BWC use by establishing effective policies and practices for its own law enforcement components. In October 2019, the Department announced a pilot program that will allow federally deputized task force officers to use BWCs while conducting arrests or executing search warrants. The OIG is currently auditing the Department's policy and practices on BWC use among its law enforcement components and federally deputized task force participants.

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.

Examples of OIG Work:

In March 2021, the OIG issued its most recent report, summarizing the OIG's Section 1001 activities from July 1, 2020, through December 31, 2020. The report described the number of complaints the OIG received under this section, the status of investigations conducted by the OIG and DOJ components in response to those complaints, and an estimate of the OIG's expenses for conducting these activities.

Specifically, during this period, the OIG processed 1,081 new complaints that were identified by the complainant as civil rights or civil liberties complaints. The OIG determined that 45 of the 1,081 complaints involved DOJ employees or DOJ components and included allegations that required further review. The OIG determined that 24 of these complaints raised management issues generally unrelated to the OIG's Section 1001 duties and referred them to DOJ components for appropriate handling.

The OIG identified 1 complaint warranting further investigation to determine whether Section 1001-related abuses occurred. The OIG referred this complaint to the BOP and requested a copy of the investigative reports upon completion of the BOP's investigation.

During this reporting period, the OIG spent approximately $48,957 in personnel costs and $100 in miscellaneous costs, for a total of $49,057 to implement its responsibilities under Section 1001. The total personnel and miscellaneous costs reflect the time and funds spent by OIG Special Agents, Attorneys, Auditors, Inspectors, Program Analysts, Paralegals, and other staff who worked directly on investigating Section 1001-related complaints, conducting special reviews, implementing the OIG's responsibilities under Section 1001, and overseeing such activities.

Ongoing Work:

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
As of March 2021, in response to requests from Members of Congress and members of the public, the OIG has initiated a review to examine the DOJ and its law enforcement components' roles and responsibilities in responding to protest activity and civil unrest in Washington, DC, and in Portland, Oregon in June and July 2020.

The review will include examining the training and instruction that was provided to the DOJ law enforcement personnel; compliance with applicable identification requirements, rules of engagement, and legal authorities; and adherence to DOJ policies regarding the use of less-lethal munitions, chemical agents, and other uses of force. About events in Lafayette Square on June 1, 2020, the OIG will coordinate our review with the Department of Interior OIG. If circumstances warrant, the OIG will consider including other issues that may arise during the review.

2. Use of Sensitive Investigative Authorities by Department Law Enforcement

The Department's law enforcement components are tasked with complex investigations, some of which have implications for national security, or involve transnational or domestic criminal enterprises. As an aid in conducting such critical investigations, components have been granted authority to use a variety of sensitive investigative techniques, including electronic surveillance, confidential sources, undercover activities, and activities that may otherwise be illegal. While using these tactics may be an effective means to disrupt national security threats or the activities of criminals, they present substantial risks to the Department.

The risks arise from reliance on the invasiveness of the techniques affecting individuals' privacy, persons with mixed motives and a history of involvement with questionable associates, activities that could endanger civilian lives, and the authorized furthering of criminal activity. Department management's challenge is to ensure appropriate controls are in place to mitigate these risks and increase the likelihood that use of sensitive investigative techniques is productive in advancing the most serious national security and criminal investigations.

The Department's Strategic Management and Oversight of Confidential Sources
Law enforcement components utilize Confidential Sources (CS) in criminal and national security investigations to identify investigative targets or infiltrate organizations representing a threat to the safety and security of our communities. However, the use of CSs is inherently risky. In FYs 2016 through 2020, the OIG reviewed the protocols for the use of CSs by the three largest Department law enforcement components, the FBI, ATF, and the DEA.

Each of these audits identified significant deficiencies in internal controls, and questionable strategic uses of CSs. Common deficiencies included a lack of oversight in the CS validation process, inability to track CS payments, and inadequate management of CS activity. To mitigate such risks, the OIG recommended the Department components that were reviewed develop and implement appropriate CS monitoring, which the Department, DEA, and ATF have since resolved and closed. The OIG remains concerned about this sensitive investigative technique and the similarity of the findings present throughout these law enforcement components.

Oversight of the Use of the Foreign Intelligence Surveillance Act
The Department's authority under the Foreign Intelligence Surveillance Act (FISA) to conduct

electronic surveillance and physical searches are a powerful investigative tool that also raises civil liberties concerns. FISA orders can be used to surveil U.S. persons, and proceedings before the Foreign Intelligence Surveillance Court (FISC) inherently exclude the party surveilled. Considering this process, the Department and FBI have established procedures and safeguards, including the requirements in FBI policy that every FISA application contain a "full and accurate" presentation of the facts and that all factual statements in FISA applications are "scrupulously accurate."

The OIG's recent work has raised serious concerns about the accuracy of the Department's submissions to the FISC and the FBI's compliance with its FISA policies and procedures. In the OIG's Review of Crossfire Hurricane, the OIG found that the FBI and Department failed to meet their basic obligation of accuracy. In four applications targeting Carter Page, a former Trump campaign advisor, the OIG found at least 17 significant inaccuracies and omissions in the applications' statements of facts supporting probable cause. As a result, relevant information was not shared with Department decision makers and the FISC, and the applications made it appear that the evidence supporting probable cause was stronger than was the case. Due to the many basic and fundamental errors that were made by separate teams on highly sensitive FISA applications (which FBI officials expected would be subjected to close scrutiny), the OIG concluded the investigation raised significant questions regarding the FBI chain of command's management and supervision of the FISA process.

3. The Department's Contingency Planning and Response to a Global Pandemic

Beginning in early-March 2020, the Office of the Inspector General (OIG) promptly shifted a significant portion of its oversight efforts toward assessing the DOJ's readiness to respond to the emerging COVID-19 pandemic. Through this assessment, and the subsequent passage of the CARES Act on March 27, 2020, the OIG determined that the most immediate challenges to DOJ operations involved preventing the spread of the virus among the roughly 155,000 federal inmates and 61,000 detainees; safely operating immigration courts; and ensuring robust oversight of $850 million in pandemic-related grant funding being disbursed to state, local, and tribal organizations. Since that time, these efforts have been expanded to include areas such as the impact of COVID-19 on DOJ law enforcement and other day to day operations.

The OIG has established an interactive dashboard relating to COVID-19 within the Federal Bureau of Prisons (BOP) linked here.

This collection of dashboards presents publicly available data obtained by the OIG from the BOP and the Johns Hopkins University's Center for Systems Science and Engineering (JHU CSSE) and is represented in various accessible formats. We are making this data available to provide further transparency to information about COVID-19 in BOP-managed correctional facilities. The dashboards will be updated each Monday.

The data as it is displayed and interpreted here should not be considered authoritative for any legal or scientific purpose. Any questions regarding the data as it is displayed and interpreted here should be directed to OIG, and not to BOP and JHU CSSE.

Examples of OIG Work:

Review of the USMS's Response to the COVID-19 Pandemic
In February 2021, the OIG released a report examining the United States Marshals Service's (USMS) response to the COVID-19 pandemic. The DOJ Office of the Inspector General (OIG) found that while the USMS has taken steps to prepare for, prevent, and manage the risks associated with COVID-19, opportunities for improvement remain.

The OIG found that the USMS's detention facility oversight plan was inconsistent and did not ensure that all active facilities were assessed for implementation of the latest Centers for Disease Control and Prevention (CDC) guidance. Facilities operated by the USMS's state and local government partners under Intergovernmental Agreements (IGA) did not receive the same scrutiny from the USMS as do the USMS contract facilities, although the IGA facilities house approximately 70% of the USMS's 61,000 prisoners. Additionally, we found that the USMS had a practice of transporting prisoners without first testing to confirm that they were COVID-19 free. We believe this practice may lead to further infections and should be re-evaluated.

The OIG made six recommendations to assist the USMS in mitigating the health risks arising from the pandemic. The USMS agreed with all six recommendations, the report can be viewed here.

Survey on the Effects of COVID-19 on ATF, DEA, FBI, USAO, and USMS Investigative Operations
In January 2021, the OIG released the results of an Interactive Survey on the effects of COVID-19 on the ATF, DEA, FBI, USAO, and USMS Investigative Operations. In conducting the anonymous online survey, the DOJ Office of the Inspector General (OIG) received more than 6,000 responses from Special Agents, criminal investigators, U.S. Marshals; Deputy U.S. Marshals, and other investigative, enforcement, and compliance personnel within the DOJ between July 7 and August 3, 2020.

The survey results describe how law enforcement personnel perceived the effects of COVID-19 on law enforcement operations and the DOJ's response to the coronavirus pandemic. The OIG's interactive dashboard allows users to view aggregate survey responses by DOJ component and by specific response, as well as see representative comments provided by the survey respondents. Results of the survey include:

- More than 64% of respondents noted that COVID-19 had affected their ability to work cases;
- 25% of respondents did not agree that their agency provided adequate personal protective equipment (PPE). Additionally, 25% of respondents indicated that their agencies' training on the use of PPE as well as how they should interact with the public and their co-workers was inadequate. Over 90% of respondents said that they had not been tested by their agency for COVID-19 as of the time of the survey;
- 62% of respondents reported always or often wearing a mask, but more than half noted federal/state partners never or only sometimes wear masks;
- Most respondents reported that they took appropriate precautions while interacting with the public during COVID-19; and,
- Most respondents indicated that protocols were in place to notify them of a positive test for individuals they had either recently worked with or taken into custody.

The OIG's survey results are intended to assist the DOJ in identifying areas of opportunity for mitigating the impact of COVID-19 (or other outbreak) on current and future Department investigative operations. The data as presented is only representative of employees who responded to our survey and should not be interpreted as representing all DOJ employees. Responses represent perceptions of survey respondents and may differ from the official policies, practices, or procedures of DOJ components.

The full report with interactive graphics can be viewed here.

Interim Report -Review of the Office of Justice Programs' Administration of CARES Act Funding

In July 2020, the OIG released a report reviewing the Office of Justice Programs' Administration of CARES Act Funding. Our preliminary objectives are to assess OJP's efforts to: (1) distribute Coronavirus award funding in a timely and efficient manner, and (2) review pre-award activities to determine if Coronavirus awards were made in accordance with applicable laws, regulations, and other guidelines.

On March 27, 2020 the U.S. Congress passed the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), providing more than $2 trillion in funding, intended to strengthen the national response to the COVID-19 global pandemic. Approximately $1.007 billion was appropriated to the Department of Justice (DOJ), with $850 million allocated to DOJ's Office of Justice Programs (OJP) to award grants for the purposes of preventing, preparing for, and responding to the Coronavirus.

OJP's Bureau of Justice Assistance (BJA) issued a solicitation for the Coronavirus Emergency Supplemental Funding grant program (CESF) on March 30, 2020. All CARES Act funding appropriated to OJP will be awarded through the CESF, which aids eligible states, U.S. territories, the District of Columbia, units of local government, and tribes.

The review indicates that OJP's administration efforts over CARES Act funding appear effective and appropriate as of May 29, 2020. However, OJP's CESF monitoring strategy may benefit if oversight protocols consider factors such as recipients who are in areas with few positive COVID-19 test results or deaths. Further, OJP should consider notifying the CESF recipient community, on a regular basis, of fraud schemes known to be targeting CARES Act funds.

The OIG made no recommendations but provided OJP a copy of the interim report for review and comment. The Office of Justice Programs (OJP) appreciates the opportunity to review and comment on this first interim report which covers OJP's actions during the Coronavirus Emergency Supplemental Funding (CESF) Program solicitation's open period. OJP commented that while the report contains no recommendations, it does provide useful monitoring strategies to mitigate the potential for fraud, waste, and abuse as the Bureau of Justice Assistance begins its oversight of an additional $850 million allocated to OJP.

Ongoing Work:

Review of the Office of Justice Programs' Administration of Coronavirus Aid, Relief, and Economic Security Act Funding

As of March 2021, the OIG initiated a review of Coronavirus Aid, Relief, and Economic Security Act funding provided through the fiscal year 2020 Office of Justice Programs' (OJP) Bureau of Justice Assistance Coronavirus Emergency Supplemental Funding Program Solicitation. The preliminary objectives are to assess OJP's efforts to: (1) distribute Coronavirus award funding in a timely and efficient manner, and (2) review pre-award activities to determine if Coronavirus awards were made in accordance with applicable laws, regulations, and other guidelines.

Remote Inspections of Facilities Housing Federal Bureau of Prisons Inmates during the COVID-19 Pandemic

As of March 2021, the OIG continues to conduct a series of remote inspections of facilities housing BOP inmates during the 2019 Novel Coronavirus Disease (COVID-19) pandemic. These inspections will assess whether BOP-managed institutions, contract institutions, and contract Residential Reentry Centers are complying with available guidance and best practices regarding preventing, managing, and containing potential COVID-19 outbreaks in correctional and residential reentry settings. The OIG's objectives include providing information gathered during these inspections to assist BOP in mitigating the health risks arising from the pandemic. As part of this work, the OIG is examining the Department's and the BOP's use of home confinement and other early release authorities provided under the CARES Act to manage the spread of COVID-19 within BOP facilities.

Review Examining BOP's Use of Home Confinement as a Response to the COVID-19 Pandemic

As of March 2021, the OIG continues a review of the Federal Bureau of Prisons' (BOP) use of home confinement as a tool to mitigate the effect of the Novel Coronavirus Disease (COVID-19) pandemic on the federal prison population. The review will assess the BOP's process for implementing the use of home confinement as authorized under the CARES Act, the process for its consideration of the eligibility criteria outlined in the Attorney General's March 26 and April 3, 2020 memoranda, and the process by which BOP headquarters evaluated wardens' recommendations that inmates who did not meet the Attorney General's criteria be placed in home confinement.

The review will also select cases for examination to determine whether there were irregularities in the BOP's processes. If circumstances warrant, the OIG will consider including other issues that may arise during the review. The OIG is undertaking this review in response to requests from Members of Congress, and issues the OIG identified during the series of remote inspections it has conducted regarding the BOP's response to the COVID-19 pandemic.

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

As of March 2021, the OIG continues to conduct a limited scope review of the Executive Office for Immigration Review's handling of certain challenges presented in conducting operations during the 2019 Novel Coronavirus Disease (COVID 19) pandemic. The OIG will assess EOIR's communication to staff, parties to proceedings, and the public about immigration court operations; its use of personal protective equipment; its use of worksite flexibilities; and its ability to mitigate health risks while maintaining operations during the COVID-19 pandemic.

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

Maintaining a safe, secure, and humane prison system remains a challenge for the Department and the BOP. The challenges the BOP has faced in the past—maintaining the overall safety of inmates, staff, and the public; interdicting contraband in its facilities; budget and staffing shortages; rising medical care costs due to an aging prison population; and long-term infrastructure maintenance—continue to impact the BOP. During 2020, the unexpected and unprecedented challenges presented by the COVID-19 pandemic exacerbated the strain on BOP. The First Step Act (FSA) of 2018 and the CARES Act of 2020 may help address some of these challenges, if the BOP is able to use effectively the authorities provided for by these laws.

From 1980 to 2013, the total number of federal inmates grew exponentially, from 24,640 to 219,298. BOP budgets rose accordingly. In a 2013 report, the OIG noted that from FY 2001 to FY 2013, BOP's budget rose from 20 percent to 25 percent of the Department's total discretionary budget. Indeed, from FY 2000 to FY 2016, the nominal per capita cost of incarcerating an inmate in the federal system increased every fiscal year from approximately $22,000 per inmate to nearly $35,000 per inmate. Consequently, even though the BOP inmate population has declined by 29 percent from 2013 to 2020 to a current total of approximately 155,000 total inmates, the BOP continues to account for fully 24 percent of the Department's total budget request in 2020.

Examples of OIG Work:

DOJ's Efforts to Protect BOP Facilities against Threats Posed by Unmanned Aircraft Systems
In September 2020, the OIG released a report on the Department's efforts to protect BOP facilities against threats posed by unmanned aircraft systems, commonly referred to as drones. Drones have been used to bring contraband to inmates, can be used to surveil the facilities, aid in escapes, or bring weapons or explosives inside the facilities. The specific findings release includes:

- Enhanced Drone Incident Tracking is Needed. Formal tracking of drone incidents within BOP began in 2018. In 2018 there were 23 incidents, and 57 in 2019. While it is a significant increase, it is believed that these numbers are under reported. The OIG found that the BOP needed improve their policies by clarifying its reporting policy for federal facilities, as well as taking steps to comprehensively track drone incidents at their contract facilities.
- Improving Drone Response Guidance. Recent flight restrictions and other legal authorities gained from 2018 to 2019 will help DOJ combat the drone threat at BOP facilities. However, delays in finalizing Department-level guidance on implementing DOJ authorities to counter drones has hampered the BOP's ability to propose and receive approval for deploying counter-drone measures and train its staff.
- Identifying and Obtaining Protective Solutions. DOJ faces several challenges in its ongoing evaluation of solutions suitable to secure BOP facilities from drone threats. These include identifying appropriate technologies, verifying that they deliver on promised capabilities, and assessing the cost and benefits of these purchases. Given the limited resources available to the BOP and the rapid evolution of technology, continued collaboration both within DOJ and among other federal agencies will be essential to addressing these challenges and protecting BOP facilities from drone threats.

This report made seven recommendations to the Department and BOP to improve BOP's tracking of drone incidents at its facilities and to promote the BOP and DOJ's efforts to protect BOP facilities against threats posed by drones. The BOP and DOJ agreed with all seven recommendations.

Remote Inspection of Federal Bureau of Prisons Contract Correctional Institution McRae, Operated by the Geo Group, Inc.

In August 2020, the OIG released a Pandemic Response Report of Federal Bureau of Prisons contract Correctional Institution McRae (McRae), operated by CoreCivic and located in McRae-Helena, Georgia. McRae houses 1,392 low security criminal alien inmates, most of which are under U.S. Immigration and Customs Enforcement (ICE) detainers, meaning that subsequent to the completion of their criminal sentence they will be transferred to ICE custody pending the completion of their removal proceedings and possible deportation. McRae has 314 correctional staff who provide daily correctional services to inmates.

McRae confirmed its first COVID-19 positive inmate case on April 2 and its first COVID-19 positive staff member on April 5. As of August 4, 18 inmates had tested positive, 2 had active cases, 15 had recovered, and 1 had died. As of August 4, an additional 7 McRae inmates had tested positive for COVID-19 and no additional inmates had died because of the disease. Telfair County, Georgia, the county in which McRae is located, had a total of 256 confirmed positive cases as of August 4.

The OIG found that McRae officials did not restrict all inmates to their housing units until 7 days after McRae identified the first inmate who presented symptoms and ultimately tested positive for COVID-19. Although McRae immediately isolated the inmate upon identification of symptoms, and had taken earlier steps to limit inmate movement throughout the institution, a McRae Physician told us that the delay in restricting the broader population of inmates to their housing units likely led to the spread of COVID-19 within the institution.

Remote Inspection of Federal Bureau of Prisons Contract Correctional Institution Giles W. Dalby, Operated by Management & Training Corporation

In August 2020, the OIG released a Pandemic Response Report of Federal Bureau of Prisons contract Correctional Institution Giles W. Dalby (Dalby), Operated by Management and Training Corporation and located in Post, Texas. Dalby houses approximately 1,439 criminal alien inmates. Most inmates at Dalby are under U.S. Immigration and Customs Enforcement (ICE) detainers, meaning that after the completion of their criminal sentence they will be transferred to ICE custody pending the completion of their removal proceedings and eventual deportation. Dalby has 267 correctional staff who provide daily correctional services to its inmates. At the time of our fieldwork, between April 29 and June 9, Correctional Institution Giles W. Dalby (Dalby), operated by MTC, had no positive COVID-19 cases. After the completion of our fieldwork, we learned that on June 22 four Dalby inmates tested positive for COVID-19. As of August 4, 83 Dalby inmates had tested positive, 8 had active cases, 74 had recovered, and 1 had died.

The OIG found that due to supply issues, for 2 weeks, Dalby was unable to comply with the April 3 CDC guideline for individuals to wear cloth face coverings in public settings where social distancing measures are difficult to maintain due to unavailability of a sufficient number of face coverings. The results of our survey of Dalby staff, conducted in May 2020, rated Dalby better than the average survey results for other contract prisons and BOP-managed institutions on

the availability of personal protective equipment (PPE), timeliness of guidance to staff, and management of potentially symptomatic inmates.

Remote Inspection of Federal Bureau of Prisons Contract Correctional Institution Moshannon Valley, Operated by the Geo Group, Inc.

In August 2020, the OIG released a Pandemic Response Report of Federal Bureau of Prisons contract Correctional Institution Moshannon Valley (Moshannon), operated by GEO Group and located in Philipsburg, Pennsylvania. Moshannon houses approximately 1,601 low security criminal alien male inmates in a facility in Philipsburg, Pennsylvania. Most inmates at Moshannon are under U.S. Immigration and Customs Enforcement (ICE) detainers, meaning that after the completion of their criminal sentence they will be transferred to ICE custody pending the completion of their removal proceedings and eventual deportation. Moshannon has 271 staff who provide daily correctional services to inmates.

At the time of our fieldwork, between April 27 and May 20, 2020, no inmates at Moshannon tested positive for COVID-19. As of August 4, there remained no inmate cases, but two staff cases. Clearfield County, the county in which Moshannon is located, had reported 142 confirmed positive COVID-19 cases.

The OIG found that due to supply issues, for over 2 weeks Moshannon was unable to comply with the April 3 CDC recommendation for individuals to wear cloth face coverings in public settings where social distancing measures are difficult to maintain. Moshannon officials adhered to all other applicable COVID-19 related BOP policies and CDC guidelines and regularly communicated changes to staff and inmates.

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

In March 2020, the OIG released the results of an audit reviewing the BOP's policies, procedures, and practices for monitoring terrorist inmates and the BOP's efforts to prevent further radicalization within its inmate population.

There were more than 500 inmates within the BOP with connections to both domestic and international terrorism. Terrorist inmates are considered high risk; due to the high-risk BOP policy requires that all communication (socially) is monitored. The OIG found that due to not accurately labeling all terrorist inmates as such there was a breakdown in appropriately monitoring their communications. The BOP started a list of soon-to-be released inmates in FY 2005 but failed to take appropriate steps to ensure that information on all formerly incarcerated terrorist inmates was provided to the FBI.

Additionally, the OIG found that due to technological limitations of the BOP's monitoring capabilities, monitoring of terrorist inmates place under a Special Administrative Measure (SAM) requiring 100-percent live communication was not being done. During the 2 years from January 2015 to December 2017, the BOP failed in their monitoring of thousands of communications of high-risk inmates. They also failed to review thousands of inmate emails, some of which contained flagging language.

The OIG made 19 recommendations to improve the BOP's accounting for, monitoring of, and security of terrorist inmates. The BOP agreed with 17 of the 19 recommendations and the Office of the Deputy Attorney General (ODAG) agreed to work with the BOP on the remaining two.

Ongoing Work:

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

As of March 2021, the OIG continues to audit the BOP's religious services program. The preliminary objective of the audit is to assess BOP's management and oversight of its religious services program to support faith-based activities and its effectiveness in preventing security risks and the misuse of program resources. This audit follows the OIG's recent audit of the BOP's Monitoring of Inmate Communications to Prevent Radicalization.

BOP's Efforts to Address Inmate Sexual Harassment and Sexual Assault against BOP Staff

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

5. Safeguarding National Security and Countering Domestic and International Terrorism

Enhancing national security and countering terrorism remain top priorities for the Department. In FY 2020, the continued mission is to prevent, disrupt, and defeat terrorist operations, prevent and neutralize weapons of mass destruction threats, address cyber threat actors, coordinate counterintelligence activities, facilitate the rapid response to crisis events, and collect intelligence to understand national security and criminal threats. As national security threats continuously change and evolve, so too must the Department's approach to combatting those threats. National Security issues relating to cybersecurity and the Management of Sensitive Investigative Authorities are discussed in separate challenges below.

Disrupting and Defeating Terrorist Operations

Among the Department's highest priorities are countering the threats posed by foreign and domestic terrorism. With respect to foreign terrorist organizations (FTO), the FBI remains focused on organizations such as al Qaeda and ISIS that have proven resilient despite setbacks and defeats. In February 2020, the FBI Director testified that, "In recent years, FTOs' use of the Internet and social media has enhanced their ability to disseminate terrorist propaganda and training materials to attract and influence individuals in the United States." In addition, in 2019 the FBI Director testified that, "Due to online recruitment, indoctrination, and instruction," FTOs no longer have to find ways to "get terrorist operatives into the country to carry out acts of terrorism."

Domestically, the United States faces threats by both homegrown violent extremists (HVE) and domestic violent extremists (DVE). HVEs are global jihad-inspired individuals who are in the United States, have been radicalized primarily in the United States, and are not receiving individualized direction from an FTO. DVEs are individuals who seek to commit violent, criminal acts to further ideological goals stemming from domestic influences, such as those of a political, religious, social, racial, or environmental nature. The FBI believes that HVEs and DVEs currently present the "greatest" terrorist threat to the United States.

Counterintelligence and Counterespionage

Foreign intelligence services seek our nation's state and military secrets. The FBI has "observed foreign adversaries employing a wide range of nontraditional collection techniques," including using individuals who are not affiliated with intelligence services to collect information, investing in critical U.S. sectors, and infiltrating U.S. supply chains. For example, a recent U.S. Senate Permanent Subcommittee on Investigations staff report criticized the FBI for responding slowly to threats posed by Chinese "talent recruitment plans," and for lacking a coordinated national outreach program to address them. The Thousand Talents Plan, the most prominent talent recruitment plan, incentivizes individuals engaged in research and development in the United States to transmit information to China.

According to the report and recent criminal prosecutions, talent recruitment plan members have downloaded sensitive electronic research files before returning to China, submitted false information when applying for grant funds, and willfully failed to disclose or lied about receiving money from the Chinese government on U.S. grant applications. The FBI Director recently described the counterintelligence and economic espionage threat from China as the "greatest long-term threat to our nation's information and intellectual property, and to our economic vitality." The Department must confront this threat by continuing to identify, investigate, and prosecute foreign adversaries and their affiliates who threaten our national security, and by providing businesses and educational institutions with the information they need to protect their own most valuable assets.

Threats to U.S. Election Security

Russia, China, Iran, and other foreign actors threaten the security of U.S. elections when they seek to interfere in the voting process or influence voter perceptions. These threats may take the form of disinformation or other social media campaigns or cyberattacks on state and local infrastructure. The Department's principal roles in combatting election interference are its counterintelligence activities in identifying, detecting, and disrupting threats to our election security, and the investigation and prosecution of federal crimes, such as violations of the Foreign Agents Registration Act and Computer Fraud and Abuse Act. According to a Deputy Assistant Attorney General of the Department's National Security Division, the Department also assists election officials, other public officials, candidates, and social media companies in "hardening their own networks, products, and platforms against malign foreign influence operations."

In FBI Director Wray's written remarks on September 17, 2020, before the House Homeland Security Committee he stated, "Our nation is confronting multi-faceted foreign threats seeking to both influence our national policies and public opinion and cause harm to our national dialogue. The FBI and our interagency partners remain concerned about, and focused on, the covert and overt influence measures used by certain adversaries in their attempts to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine the American people's confidence in our democratic processes." Furthermore, the Directors of the FBI, National Security Agency, Cybersecurity and Infrastructure Security Agency, and National Counterintelligence and Security Center issued a joint message on October 6, 2020, discussing their agencies' commitment and methods to protect and ensure the integrity of the 2020 election.

Combatting Insider Threats and Unauthorized Disclosures

In accordance with its 2018-2022 Strategic Plan, the Department must continue to protect itself against insider threats and potential leaks of sensitive information. The Department recently has

prosecuted insiders who allegedly made unauthorized disclosures of sensitive information. These insiders have included a Defense Intelligence Agency counterterrorism analyst who pleaded guilty in connection with charges that he provided classified national defense information to two members of the news media, and a former federal government employee and contractor who pleaded guilty in connection with charges that she improperly retained a classified document that outlined intelligence information. The Department has also prosecuted government insiders, including former CIA officers, for sharing or attempting to share information with our foreign adversaries as part of our adversaries' espionage and intelligence-gathering efforts.

In 2017, the OIG issued a report on its audit of the FBI's insider threat program. We made eight recommendations to improve the FBI's program for deterring, detecting and mitigating malicious insider threats, including recommendations that the FBI ensure insider threat leads are handled and monitored in a systematic way, and that all classified systems and networks have user activity monitoring coverage. The FBI concurred with all our recommendations. More recently, the OIG initiated an audit that will assess the FBI's internal controls related to the physical security of covert video and audio equipment and data under a contract awarded by the FBI to a third party.

Examples of OIG Work:

Notification of Concerns Identified in the Federal Bureau of Investigation's (FBI) Contract Administration of a Certain Classified National Security Program

In September 2020, the OIG released a Management Advisory with the purpose of advising the FBI of the conclusion of the OIG's review of the FBI's contracts awarded for a certain classified national security program. The objectives were to evaluate the FBI's awarding and administration of the contracts for this program, and to evaluate their procedures and processes for ensuring contractor performance and compliance with the terms, conditions, laws, and regulations applicable to these contracts.

The OIG held an exit conference with the FBI and provided the FBI with a copy of the working draft report. In the report several concerns were identified with the FBI's administration of these national security contracts. The working draft listed 11 recommendations for the FBI to improve its procedures and practices related to contract administration associated to this and other national security programs, as applicable.

We recognize based on our discussion at the exit conference and the FBI's written comments that concerns remain about the specific language of some of the OIG's 11 recommendations. In view of the unusual circumstances affecting this review, we will work with the FBI to ensure that each of these recommendations can be addressed consistent with the original intent of the recommendation and the FBI's ability to reasonably implement corrective actions. Because of the Top Secret marking of the working draft report pending the FBI's classification review, it cannot be released publicly. However, the OIG will release an unclassified public statement explaining that we have concluded this review

Audit of the Federal Bureau of Investigation's Efforts to Identify Homegrown Violent Extremists through Counterterrorism Assessments

In a March 2020 OIG report, the OIG found the FBI had not taken sufficient action to resolve certain weaknesses in its process for assessing potential HVEs and lacked comprehensive strategies to mitigate emerging challenges related to assessing potential HVEs. While the FBI conducted reviews following HVE attacks that identified the need for the FBI to improve its process for assessing counterterrorism threats and suspicious activities, we found the FBI did not ensure field offices implemented the changes and best practices recommended. Additionally, the FBI conducted an enterprise-wide evaluation of its database for tracking and managing threats and recommended additional investigative action in 6 percent of counterterrorism assessments closed between 2014 and 2016. However, we found the FBI did not ensure field offices took appropriate action to address these investigative deficiencies.

As a result, nearly 40 percent of these counterterrorism assessments went unaddressed for 18 months after deficiencies were known. We further found the FBI needs to provide adequate guidance and training to field offices to appropriately and consistently handle challenges associated with the crossover between terrorist threats and other categories of threats, such as criminal threats to life that do not have a national security nexus and threats posed by persons with mental health issues. While the FBI has made combatting HVEs one of its top priorities, more work must be done. We made seven recommendations to assist the FBI in its efforts to identify HVEs through counterterrorism assessments. The FBI's response to our recommendations will assist the Department's efforts to address this "greatest threat" to the nation. As such, the FBI has been working with the OIG since the issuance of the report to implement the necessary corrective actions to close the seven recommendations.

Ongoing Work:

FBI's National Security Undercover Operations

As of March 2021, the OIG continues to audit of the FBI's National Security Undercover Operations. The preliminary objectives are to evaluate: (1) the FBI's oversight of national security-related undercover operations, and (2) the FBI's efforts to recruit and train agents for these undercover operations.

Review Examining the Role and Activity of DOJ and its Components in Preparing for and Responding to the Events at the U.S. Capitol on January 6, 2021

As of March 2021, the Office of the Inspector General (OIG) initiated a review to examine the role and activity of DOJ and its components in preparing for and responding to the events at the U.S. Capitol on January 6, 2021. The OIG will coordinate its review with reviews also being conducted by the Offices of Inspector General of the Department of Defense, the Department of Homeland Security, and the Department of the Interior.

The OIG review will include examining information relevant to the January 6 events that was available to DOJ and its components in advance of January 6; the extent to which such information was shared by DOJ and its components with the U.S. Capitol Police and other federal, state, and local agencies; and the role of DOJ personnel in responding to the events at the U.S. Capitol on January 6.

The OIG also will assess whether there are any weaknesses in DOJ protocols, policies, or procedures that adversely affected the ability of DOJ or its components to prepare effectively for and respond to the events at the U.S. Capitol on January 6. If circumstances warrant, the OIG will consider examining other issues that may arise during the review.

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.

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

Cyber-related threats have the potential to adversely impact the national security and the domestic economy. As both a law enforcement agency and a member of the Intelligence Community, the Department has an integral role in protecting the nation against these threats. Moreover, as a repository of classified national security information, law enforcement sensitive information, and other sensitive but unclassified information, the Department must ensure that its own information systems are secure in the face of cyber-related threats.

The Department will be challenged to sustain a focused, well-coordinated cybersecurity approach for the foreseeable future. Cybersecurity is a high-risk area across the federal government and the Department must continue to emphasize protection of its own data and computer systems, while marshalling the necessary resources to combat cybercrime and effectively engaging the private sector.

For example, the OIG's Cyber Investigation Office (Cyber) is currently investigating an international fraud scheme where the subjects are impersonating current DOJ procurement officials and senior leaders at the Department and other federal agencies in order to submit fraudulent purchase orders to domestic businesses. Believing these are legitimate purchase orders from DOJ, the businesses ship laptops, overhead projectors, and other Information Technology (IT) products to storage locations in the U.S. where it is collected by a co-conspirator and shipped overseas.

In October 2019, OIG Cyber Agents seized over $1.3 million of fraudulently obtained IT Information Technology equipment (laptops, hard drives, projectors, etc.) at an Air Cargo business located at JFK Airport. These stolen goods were destined for Nigeria and were intercepted by OIG and returned to the victim companies, including small businesses that were tricked into shipping the goods and trusting that they were destined for U.S. Government Agencies who would pay for the products upon receipt. Once the goods were shipped to Nigeria the victim companies would not be paid.

Digital Forensics and Cyber Crime Investigations

Cyber continues to conduct computer forensic examinations and mobile device forensic examinations for over 500 pieces of digital evidence annually, which includes computers, hard drives, cell phones, tablets, and other electronic media. These examinations support over 100 OIG investigations each year. Cyber reviews numerous referrals from the Justice Security Operations Center (JSOC) regarding the leak or spillage of Personally Identifiable Information and other sensitive DOJ data, to include insider threat allegations, and makes appropriate investigative disposition in consultation with Investigations Division senior officials.

Cyber Special Agents continue to investigate cyber-crime and insider threat matters, as well as attempted intrusions into the Department's network, spoofing of Department emails to

accomplish criminal activity, and impersonation of Department officials in furtherance of fraud schemes. In addition, Cyber staff handle numerous eDiscovery requests for OIG, to include FOIA, Litigation Holds and Civil matters, as well as provide technical investigative equipment support for Division Field Offices to include consensually monitored calls and installation of cameras or recording devices for undercover operations.

Insider Threat Prevention and Detection Program

The Insider Threat Prevention and Detection Program (ITPDP) is designed to deter, detect, and mitigate insider threats from DOJ employees and contractors who would use their authorized access to do harm to the security of the U.S., which can include damage through espionage, terrorism, unauthorized disclosure of information, or through the loss or degradation of departmental resources or capabilities.

There are two parts to the OIG's role in the DOJ ITPDP. One is compliance with DOJ Order 0901 that requires the OIG to work with the Department in its efforts to monitor user network activity relating to classified material and networks. The reporting, training, and coordination requirements in this first role are being implemented by Management and Planning Division's Office of Security Programs. The second part of the ITPDP involves the OIG's Cyber office, which has representatives who act as law enforcement liaisons to the ITPDP relating to Insider Threat referrals.

Cyber Special Agents are currently conducting a high-profile Insider Threat investigation, which involves international companies and highly sensitive matters. This investigation alone has resulted in the guilty plea of a former DOJ employee, a non-DOJ employee and the seizure of over $73 million. Due to its unique skill set and capabilities, Cyber Agents are also working with the FBI on instances where DOJ employees were alleged to have been in attendance at the Capitol Riots that took place on January 6, 2021.

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 (DHS) 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 2020 FISMA results were submitted to OMB by November 2, 2020. The OIG reviewed compliance at six DOJ components: the FBI, JMD, ATF, Civil Rights Division, National Security Division, and USMS; and at the Court Services and Offender Supervision Agency, an independent, federal executive branch agency.

Examples of OIG Work:

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

In December 2020, the OIG released an audit of the FBI's strategy and efforts to disrupt illegal dark web activities. The preliminary objective was to assess the implementation of the FBI's dark web strategy.

The terms "dark web" and "darknet" are often used to refer to a part of the Internet that consists of services and websites that cannot be accessed through standard web browsers; instead, specific software, configurations, or authorization is needed for access. While accessing the dark web is not illegal, dark web sites are often used to engage in illegal activities.

We found that the FBI does not maintain an FBI-wide dark web strategy. Instead, the FBI relies on its operational units to execute individual dark web investigative strategies. The OIG concluded that this strategy could be enhanced by establishing a coordinated FBI-wide dark web approach helping to ensure clarity on investigative responsibilities among operational units. This could lead to more efficient and cost-effective investigative tool development and acquisition, also providing strategic continuity during turnover periods. In addition to enhancing their FBI-wide dark web strategy they should also complete an FBI-wide cryptocurrency support strategy.

The OIG made five recommendations to assist the FBI in improving its efforts related to the dark web. The FBI concurred with the five recommendations made by the OIG.

Audit of the Tax Division's Information Security Program Pursuant to the Federal Information Security Modernization Act of 2014 Fiscal Year 2019

In March 2020, the OIG released and audit determining whether the Tax Division's information security program and practices were consistent with FISMA requirements. The audit was also designed to complete the DHS FY 2019 Cyberscope reporting metrics.

The OIG found weaknesses in four of the eight domain areas in need of enhancement to ensure the Tax Division's information systems and data are properly protected. To make the Tax Division leadership aware of the findings, the auditors presented them prior to this report being released. Tax Division senior leadership agreed with the OIG findings and recommendations.

Management Advisory Memorandum of Concerns Identified with the Federal Bureau of Prisons' Compliance with Department of Justice Requirements on the Use and Monitoring of Computers, Cybersecurity, and Records Retention

In March 2020, the OIG issued a MAM to the Director of the BOP identifying concerns with the BOP's compliance with DOJ requirements on the use and monitoring of computers, cybersecurity, and records retention.

During investigations involving administrative misconduct by BOP personnel, the OIG discovered that the BOP: (a) has not developed, documented, and implemented rules of behavior for employees when accessing and using DOJ electronic systems, as required by DOJ policy; (b) has not required all mobile device users to review and agree to the standard DOJ General Rules of Behavior (ROB) agreement and to any additional BOP specific rules, as required by DOJ policy; (c) has placed a "personal container" on BOP-issued mobile devices but has not created a list of approved, vetted Apps that may be used within the "personal container," as required by DOJ policy; and (d) has not trained mobile device users on the security risks associated with

downloading unvetted Apps onto BOP-issued devices and has not instituted controls that restrict users from installing Apps on BOP-issued devices that are on the DOJ Prohibited Apps list, as required by DOJ policy.

Additionally, during the investigation it was learned that a BOP employee misused her BOP issued mobile device when she (1) used her device to send sexually explicit photographs of herself, and (2) intentionally downloaded and used encrypted communication applications, i.e. "chat" applications. During the interviews it was learned that the BOP did not prohibit or restrict BOP employees from downloading encrypted chat applications and has not instituted restricting controls on their devices.

The OIG made four recommendations to properly train personnel and protect devices. On July 21, 2020, the BOP responded to the OIG's March 2020 MAM. The OIG is currently reviewing the BOP's response to the four recommendations for compliance and sufficiency.

Ongoing Work:

Fiscal Year 2020 – Annual Information Technology Security Evaluation Pursuant to the Federal Information Security Modernization Act

As of March 2021, the OIG continues to conduct its annual Federal Information Security Modernization Act (FISMA) evaluation for fiscal year (FY) 2020. FISMA requires that the OIG, or independent evaluators selected by the OIG, perform an annual independent evaluation of the Department of Justice's (Department) information security programs and practices. The OIG will also review select systems from each component to assess the effectiveness of the Department's information security programs and practices.

7. The Opioid Crisis, Violent Crime, and the Need for Strong Law Enforcement Coordination

The past year has seen progress and setbacks in the areas of the opioid epidemic and violent crime. While nationwide violent crime declined in 2018 and the first 6 months of 2019, FBI statistics reflect a 15 percent increase nationally, between 2019 and 2020. The opioid epidemic has been complicated by the COVID-19 pandemic during 2020. After drug overdose deaths declined for the first time in 25 years in 2018, they rose again in 2019, and are currently on track to rise substantially in 2020. Critical to addressing these two enforcements and community priorities is coordination among law enforcement agencies. As the nation's leading law enforcement agency, and supporter of local law enforcement efforts, this is one of the significant challenges that the Department continues to face.

Law Enforcement Coordination and Information Sharing

Information sharing among federal agencies is an ongoing challenge. For example, as noted in the OIG's FY 2019 TMPC Report, a July 2019 joint DOJ and Department of Homeland Security OIG review of law enforcement cooperation on the Southwest border found a lack of information sharing policies between the FBI and Homeland Security Investigations (HSI), resulting in over one-third of special agent survey respondents reporting at least one cooperation failure between agencies, a range of deconfliction and information sharing issues that required attention, special agents lacking an understanding of the other agency's mission and authorities, and many agents lacking trust in the other agency or its personnel.

This review made five recommendations to improve cooperation between the FBI and HSI. Further indicative of the lack of coordination between these two federal agencies is that more than a year after issuance of the joint report, the key recommendation, requiring a memorandum of understanding between FBI and HSI on information sharing and coordination, remains open. Although the FBI has agreed with the recommendation, HSI has not concurred.

The Opioid Crisis

After rising every year for 25 consecutive years, drug overdoses declined slightly in 2018, only to increase by 4.8 percent in 2019 and set a new record high of nearly 73,000 deaths in the 12-month period ending in February 2020. Although the DEA initially reduced the annual quota for opioids in 2020, the public health emergency of the coronavirus pandemic led to a reversal of this decision, as well as other policy changes that were intended to ensure availability of opioids for ventilator patients stricken with COVID-19 and other patients who suddenly lacked direct access to doctors and clinics.

A May 13, 2020 report by the Office of National Drug Control Policy shows an 11.4 percent year-over-year increase in fatalities for the first 4 months of 2020, and an increase of 18.6 percent for non-fatal overdoses during that time frame. If the current trend of overdose deaths continues through 2020, it will be the sharpest annual increase since 2016, when the synthetic opioid, fentanyl, first made significant inroads into the country.

In September 2020, the OIG issued a report on the DEA's community-based efforts to combat the opioid crisis. Since 2016, the DEA has deployed in 20 "pilot cities" its "360 Strategy," which brings together U.S. Attorney's Offices, state and local law enforcement, educators, prevention and treatment providers, and other entities to reduce the impact of opioid misuse and addiction. Taking these actions to enhance coordination with their state and local counterparts, as well as health care professionals, was an important step forward by the DEA. The OIG report found, however, that despite multiple oversight efforts, the DEA still lacks an outcome-oriented performance measurement strategy to assess the effectiveness of its 360 Strategy. Consequently, the OIG recommended that the DEA develop clearly defined goals prior to project implementation and include a focus on sustainability. We further recommended that the DEA enhance its pilot city selection process by supplementing its use of CDC data with broader information.

Violent Crime

Ensuring the safety of our communities by reducing violent crime continues to be a critical challenge for the Department. While the U.S. violent crime rate is nearly half of what it was at the 1992 peak, violence remains a persistent problem for many communities. Between 2014 and 2016, homicides increased 20 percent, the highest rate of increase in 49 years. Since then, the Department's FY 2019 Performance Report indicated that it achieved 11 of its 13 FY 2019 targets for reducing violent crime and promoting public safety. However, in 2020, there has been a substantial increase in violence in many cities.

Additionally, the FBI reports that hate crimes against minority groups continue to rise. Indeed, the FBI Director has testified that the "top threat we face from domestic violent extremists stems from those we identify as racially/ethnically motivated violent extremists." The pandemic has heightened these concerns and prompted legislation to be introduced in Congress to combat COVID-19 hate crimes. As always, the challenge is to focus the most effective law enforcement efforts and violence reduction programs in the areas that need them most.

In FY 2020, the Department launched Operation Relentless Pursuit, an initiative aimed at combatting violent crime, through a surge of federal resources, in seven cities experiencing increasing levels of violence. This initiative was subsumed into Operation Legend, which sought to also involve state and local law enforcement officials in this effort. Since the latter operation's launch, through August 31, 2020, more than 2,000 arrests have been made, including 147 for homicide. This initiative is still ongoing.

Examples of OIG Work:

Audit of the Drug Enforcement Administration's Community-Based Efforts to Combat the Opioid Crisis

In September 2020, the OIG released a report examining the Drug Enforcement Administration's (DEA) community-based efforts to combat the opioid crisis.

The OIG found the DEA had deployed its 360 Strategy, a program intended to combat opioid abuse, in 20 communities across the U.S., where it helped to increase awareness of opioid-related issues, provide training, build anti-drug coalitions, and create online resources available to the public at no charge. There were some areas identified for improvement in the DEA's pilot city selection process, allocation of resources, and collaborative efforts with other federal entities tasked with combatting the opioid crisis. Despite multiple oversight efforts, the DEA still lacks an outcome-oriented performance measurement strategy to assess the effectiveness of its community outreach efforts, and we identified potential opportunities to reduce misconceptions surrounding medication-assisted treatment. The OIG's specific findings in this report include:

- DEA Can Improve How it Uses Data to Allocate its Resources: We found that a review of DEA field data, which analyzes substances such as fentanyl from an availability and seizure standpoint, would strengthen the DEA's ability to ensure its resources are deployed to communities most in need of opioid-related assistance.
- DEA Should Enhance its Outcome-Oriented Performance Measurement Strategy: We found that the DEA lacks effective outcome-oriented performance measurements, an issue also identified in our 2003 Audit of the DOJ Drug Demand Reduction Activities.
- DEA Would Benefit From a Comprehensive Review of its Opioid-Related Media Efforts: The DEA has not consistently established performance metrics to assess the impact of its community outreach efforts, referred to as "Wake Up," and has struggled to generate significant public traffic to the websites where the resources are provided.
- DEA Should Enhance its Collaborative Efforts with Other Entities Situated to Provide Opioid-Related Assistance: We found that the DEA's collaborative efforts with DOJ grant making agencies are limited. These agencies provide millions of dollars in opioid-related funding to community organizations and local law enforcement across the United States each year. Enhanced collaboration with these agencies may improve DEA's long-term efforts to sustain progress in the communities it assists.

This report contains five recommendations to the DEA to enhance the DEA's community-based efforts to combat the opioid crisis. The DEA agreed with all the recommendations.

8. Ensuring Financial Accountability of Department Contracts and Grants

In FY 2020 the Department awarded approximately $8.5 billion in contracts and over $4.9 billion in grants. The passage of the CARES Act in March 2020 provided $1 billion in funding

to the DOJ for addressing the COVID-19 pandemic, of which $850 million is being administered by OJP. Oversight of all contracts and grants awarded to ensure financial accountability and mitigate the risks of fraud or misuse of contract and grant funds is an ongoing challenge. The Department faces an added challenge in connection with the CARES Act awards because of the urgent need to have made the awards promptly.

Examples of OIG Work:

Audit of the Office of Justice Programs Victim Assistance Grants Awarded to the Florida Department of Legal Affairs (FDLA), Tallahassee, Florida
In September 2020, the OIG released a report auditing four Victims of Crimes Act (VOCA) victim assistance formula grants awarded by the Office of Justice Programs (OJP) Office for Victims of Crimes (OVC) to the FDLA in Tallahassee, Florida. The formulas grants totaled more than $582 million for FYs 2015 to 2018. The OIG evaluated how the Florida Department of Legal Affairs (FDLA) designed and implemented its crime assistance program. This was done by assessing their performance in the following areas: (1) grant program planning and execution, (2) program requirements and performance reporting, (3) grant financial management, and (4) monitoring of subrecipients.

The OIG concluded that the FDLA successfully provided services to crime victims through their subrecipients; but they did not utilize available funds to assist more crime victims. In FY15 and FY16, the FDLA returned $2.2 million and $57.3 million respectively to OJP. We approximate that the FDLA may need to return $172.5 million of their 2017 and 2018 awards when the expire. The OIG identified area of the FDLA's grant management that could be improved, specifically the grant financial management. Additionally, the FDLA did not have grant funds draw down procedures from OJP.

Audit of the Office of Justice Programs Victim Assistance Grants Awarded to the New Jersey Department of Law and Public Safety, Trenton, New Jersey
In July 2020, the OIG released a report evaluating how the New Jersey Department of Law and Public Safety (NJ DLPS) designed and implemented its crime victim assistance program. There were four areas that were assessed to accomplish this objective: (1) grant program planning and execution; (2) program requirements and performance reporting; (3) grant financial management; and (4) monitoring of subrecipients.

The OIG concluded that NJ DLPS did not meet all of the grant requirements regarding: (1) obligating and expending funds within the project period; (2) awarding funds to subrecipients in a timely manner; (3) monitoring compliance with priority area funding requirement; (4) ensuring annual performance reports were complete and accurate; (5) administering and monitoring subrecipient awards; and 6) awarding funds to sub recipients in a timely manner. There was also approximately $74,000 in questionable costs. Despite these discrepancies the OIG found NJ DLPS conducted adequate strategic planning and increased the number of projects funded and scope of services provided had an adequate financial management system in place.

The OIG made seven recommendations to OJP to assist NJ DLPS in improving its grant management and administration, and to remedy questioned costs. The NJ DLPS agreed with all seven recommendations and concluded that given the extent of the work required to comply with

the recommendations that it may take up to 12 months or more to complete these recommendations.

Audit of the Office of Community Oriented Policing Services Hiring Program Grants Awarded to the Arlington Police Department, Arlington, Texas
In June 2020, the OIG released a report where they audited three grants totaling $11.2 million in project costs that included $5.6 million in federal funds for the Community Oriented Policing Services (COPS) Hiring Program (CHP) within the Arlington Police Department (APD). The objectives were to determine whether: (1) costs claimed were allowable, supported, and in accordance with applicable laws, regulations, guidelines and terms and conditions of the award; and (2) the grantee demonstrated adequate progress towards achieving program goals and objectives.

The OIG concluded the following: (1) The APD demonstrated adequate progress toward achieving the grants' stated community policing goals, except that the APD did not provide documentation of activity with what it considered its three most important partners under the grant; (2) We did not identify significant concerns regarding the APD's required match and application statistics. However, we identified noncompliance with essential award conditions related to performance reports, officer type, use of funds, and financial accounting; (3) The APD charged unallowable salaries for ineligible officers to the grants, charged unallowable salaries and fringe benefits over the approved amounts in the Financial Clearance Memorandums (FCM), and did not accurately account for grant expenditures by cost category; and 4) We determined that procedures related to progress reports, budget management and control, drawdowns, and federal financial reporting could be improved. As a result of these deficiencies, we identified over $878,000 in unallowable total project costs. The APD repaid the federal share to DOJ before the issuance of this final report.

The OIG made 13 recommendations to the COPS Office of which the APD agreed with all of them.

Ongoing Work:

Audit of Contracts Awarded for Covert Contracts
As of March 2021, the OIG continues to conduct an audit of the FBI's National Security Undercover Operations. The preliminary objectives are to evaluate: (1) the FBI's oversight of national security-related undercover operations, and (2) the FBI's efforts to recruit and train agents for these undercover operations.

Audit of the Federal Bureau of Prison's Contracts Awarded to the University of Massachusetts Medical School
As of March 2021, the OIG continues to conduct an audit of the BOP's comprehensive medical services contracts awarded to the University of Massachusetts Medical School (UMass). The preliminary objective of the audit is to assess BOP's administration of the contracts, and UMass' performance and compliance with the terms, conditions, laws, and regulations applicable to these contracts. The assessment of performance may include financial management, monitoring, reporting, and progress toward meeting the contract goals and objectives.

9. Strategic Planning: The Department's Challenges to Achieve Performance-Based Management and to Enhance Human Capital

Pursuant to the Government Performance and Results Modernization Act of 2010 (GPRA Modernization Act), the Attorney General established four strategic goals in the DOJ FY 2018-2022 Strategic Plan. One of these goals encompasses promotion of "good government," which has as its objectives the achievement of management excellence, workforce development, and deployment of innovative technology.

The Department's Challenge to Achieve Performance-Based Management

Performance-based management involves using reliable statistics and narratives to ensure programs are achieving set goals and contributing to the overall mission of the Department. Despite the critical nature of utilizing performance data, many Department components lack either meaningful performance measures or the data necessary to evaluate their programs.

In a September 2020 report, the OIG found that between 2016 and 2019, the DEA deployed its 360 Strategy in 20 communities across the U.S., where it has helped to increase awareness of opioid-related issues, provide training, build anti-drug coalitions, and create online resources available to the public at no charge. While these are positive strides, the OIG found that the DEA needs to improve performance metrics to assess the value and effectiveness of the community-based efforts undertaken as part of its 360 strategy.

Similarly, in a June 2020 review the OIG found that although the DEA identified certain undercover operations as one of its most successful tools, the DEA did not track operational achievements in a way that allowed DEA management, the Department, or Congress to understand whether operations successfully completed the authorized objectives and goals, built cases that led to prosecutions, and deprived criminals of ill-gotten gains. We also found that the DEA did not always leverage information or strategically evaluate connections between these undercover operations.

The Department's Challenge to Enhance Human Capital

To achieve the goal of "good government" as identified in the DOJ Strategic Plan, one of the Department's strategies are to employ, develop, and foster a collaborative, qualified, high-performing, and diverse workforce. The 2019 Federal Viewpoint Survey (FEVS) results highlight that the Department scored poorly in several categories, causing the Department's ranking among best places to work among the large federal agencies to decline from 2015 to 2019.

Some of the FEVS categories include effective leadership, work-life balance, support for diversity, training and development, and performance-based rewards and advancement. A low FEVS ranking reflects and impacts the Department's ability to recruit and retain employees. Although the Department's mission remains a strength, the market for top talent is highly competitive. Thus, in furtherance of its goal of employing a high performing and diverse workforce, the Department and each component should take action to improve in each of the FEVS categories reflected.

10. Whistleblower Protection Coordinator Program

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

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

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

- Educating DOJ employees and managers about prohibitions on retaliation for protected disclosures;
- Educating employees who have made or are contemplating making a protected disclosure about the rights and remedies available to them;
- Ensuring that the OIG is promptly and thoroughly reviewing complaints that it receives, and that it is communicating effectively with whistleblowers throughout the process; and
- Coordinating with the OSC, other agencies, and non-governmental organizations on relevant matters.

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

The DOJ OIG also continues to utilize the tracking system developed through the OIG Ombudsperson Program to ensure that it is handling these important matters in a timely manner. The DOJ OIG continuously enhances the content on its public website, oig.justice.gov. The table below, pulled from our *Semiannual Report to Congress, April 1, 2020 through September 30, 2020,* presents important information.

Whistleblower Program
April 1, 2020 – September 30, 2020

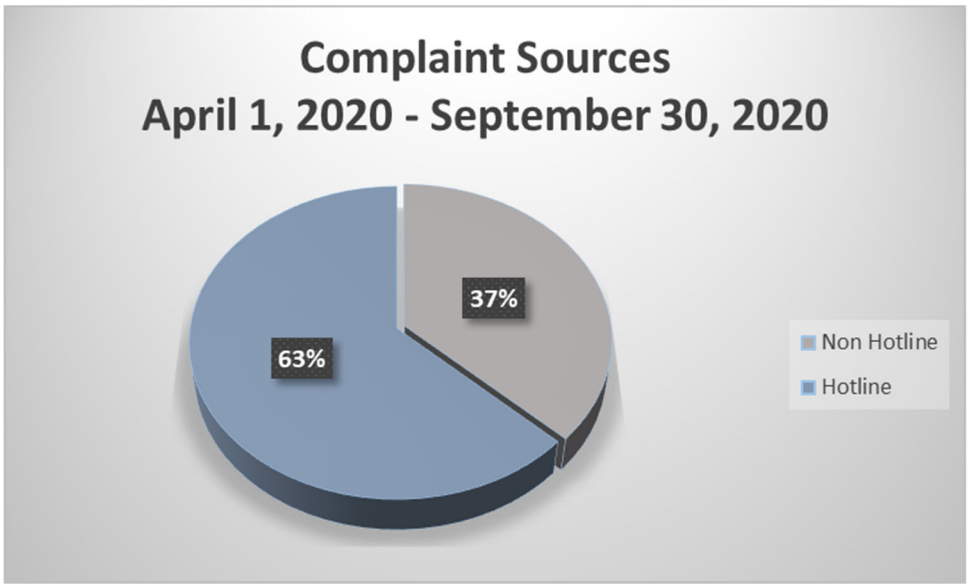
Employee complaints received	223
Employee complaints opened for investigation by the OIG	62
Employee complaints that were referred by the OIG to the components for investigation	98
Employee complaint cases closed by the OIG	84

The DOJ OIG continues to refine its internal mechanisms to ensure prompt reviews of whistleblower submissions and communication with those who come forward with information in a timely fashion.

11. OIG Hotline

During FY 2020, the OIG received most of its Hotline complaints through its electronic complaint form located here.

In addition, DOJ employees and citizens can file complaints by telephone, fax, and postal mail. The online access, fax, and postal mail all provide the ability to file a complaint in writing to the OIG.
From all Hotline sources during the second half of FY 2020, 5,531 new complaints related to DOJ operations or other federal agencies were entered into the OIG's complaint tracking system. Of the new complaints, 3,989 were forwarded to various DOJ components for their review and appropriate action; 523 were filed for information; 881 were forwarded to other federal agencies; and 9 were opened by the OIG for investigation.



12. Congressional Testimony

The Inspector General testified before Congress on the following occasions:

- "Management, Performance Challenges, and COVID Response at the Department of Justice" before the U.S. House of Representatives, Subcommittee on Commerce, Justice, Science and Related Agencies on March 24, 2021;
- "Accountability and Lessons Learned from the Trump Administration's Child Separation Policy" before the U.S. House of Representatives Committee on Oversight and Reform on February 4, 2021;
- "Protecting Those Who Blew the Whistle on Government Wrongdoing" before the House Committee on Oversight and Reform on January 28, 2020;
- "DOJ OIG FISA Report: Methodology, Scope, and Findings" before the U.S. Senate Committee on Homeland Security and Governmental Affairs on December 18, 2019;
- "Examining the Inspector General's Report on Alleged Abuses of the Foreign Intelligence Surveillance Act" before the U.S. Senate Committee on the Judiciary on December 11, 2019;

13. Support for the Department's Savings and Efficiencies Initiatives

In support of DOJ's $AVE initiatives, the OIG contributed to the Department's cost-saving efforts in FY 2020, as follows:

- *Increasing the use of self-service online booking for official travel.* Through September 2020, the OIG's on-line booking rate for FY 2020 official travel was 92 percent for a savings of $19,174 over agent-assisted ticketing costs. Online reservations cost $9.35 per transaction, compared to $37.63 per agent-assisted transaction.

- *Using non-refundable airfares rather than contract airfares or non-contract refundable fares (under appropriate circumstances).* Through September 2020, the OIG realized cost savings of $1,135. Non-refundable tickets should be considered when the cost is lower than the contract fare, and there is a high degree of certainty that cancellation or changes in travel arrangements will not be necessary. The OIG has the potential to achieve substantial cost savings from non-refundable tickets, so use of non-refundable fares is encouraged as mission permits.

- *Increased use of video conferencing*. The OIG saved training and travel dollars, as well as productive staff time while in travel status, by utilizing increased video teleconferencing and online video capabilities for all applicable OIG-wide training and meetings. Getting the most from taxpayer dollars requires ongoing attention and effort. The OIG continues to look for ways to use its precious resources wisely and to examine how it does business to further improve efficiencies and reduce costs.

E. Challenges

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

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

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

II. Summary of Program Changes

Item Name	Description	Pos.	FTE	Dollars ($000)	Page
Information Technology Division Enhancement	The OIG requests a program enhancement to ensure its IT Cloud infrastructure is agile enough to respond to unforeseen events like the COVID-19 pandemic and durable enough to withstand the gradually increasing demand due to the evolving complexity and volume of OIG oversight work.	0	0	$2,900.00	45
Physical Infrastructure Modifications to Ensure Productivity Post-Pandemic	The OIG requests a program enhancement for the design, construction, certification, and maintenance of SCIFs and other capabilities to ensure the OIG continues providing high quality oversight of the DOJ's national security programs.	0	0	$2,950.00	48
Total		**0**	**0**	**$ 5,850.00**	

III. Appropriations Language and Analysis of Appropriations Language

The appropriation language states the following for the OIG:

For necessary expenses of the Office of Inspector General, $127,184,000 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, 2023.

(Department of Justice Appropriations Act, 2021)

Provided, That notwithstanding section 1402(d) of such Act, of the amounts available from the Fund for obligation: (1) $10,000,000 shall be transferred to the Department of Justice Office of Inspector General and remain available until expended for oversight and auditing purposes of any crime victim-related programs, grants, or services; 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. Provided, That funds appropriated to the Department of Justice Office of Inspector General under sections 510 of Division B of Public Law 116-260 and Public Law 116-93 may be used by the Department of Justice Office of Inspector General for oversight and auditing purposes of any crime victim-related programs, grants, or services.

A. Analysis of Appropriations Language

No proposed changes.

IV. Program Activity Justification

A. Audits, Inspections, Investigations, and Reviews

Program Increases

OIG	Direct Pos.	Direct FTE	Amount
2020 Enacted	482	505	$105,000
2021 Enacted	491	466	$120,565
Adjustments to Base and Technical Adjustments	48	63	$10,769
2022 Current Services	539	529	$131,334
2022 Program Increases	0	0	$5,850
2022 Request	539	529	$137,184
Total Change 2021-2022	48	63	$16,619

OIG Information Technology Breakout	Direct Pos.	Direct FTE	Amount
2020 Enacted	26.0	26.0	$10,834
2021 Enacted	26.0	26.0	$15,566
2022 Current Services	29.0	29.0	$11,641
2022 Program Increase	0.0	0.0	$2,900
2022 Request	29.0	29.0	$14,541
Total Change 2021-2022	0.0	0.0	($1,025)

B. Program Description

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

C. Performance and Resource Tables

PERFORMANCE AND RESOURCES TABLE (Goal 1)												
Decision Unit: OIG/Audits, Inspections, Investigations, and Reviews												
DOJ Strategic Plan: Strategic Objective 4.1: Uphold the rule of law and integrity in the proper administration of justice.												
OIG General Goal #1: Detect and deter misconduct in programs and operations within or financed by the Department.												
WORKLOAD/RESOURCES	**FY2019**		**FY2020**				**FY2021**				**FY2022**	
	Actuals		**Projected**		**Actuals**		**Projected**		**Actuals 1st Qtr**		**Projected**	
Total Costs and FTE	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
(reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total)	442 69	$101,000 [$14,120]	490 27	$105,000 [$14,669]	505 25	$105,000 [$14,669]	466 68	$120,565 [$15,051]	466 68	$120,565 [$15,051]	514 20	$137,184 [$15,255]
Performance Measure												
Number of Cases Opened per 1,000 DOJ employees:												
Fraud*		0.49		*		0.56		*		0.09		*
Bribery*		0.16		*		0.10		*		0.06		*
Rights Violations*		0.15		*		0.10		*		0.00		*
Sexual Crimes*		0.19		*		0.21		*		0.03		*
Official Misconduct*		1.05		*		0.86		*		0.18		*
Theft*		0.05		*		0.06		*		0.01		*
Workload												
Investigations closed ##		243		N/A		N/A		N/A		N/A		N/A
Integrity Briefings/Presentations to DOJ employees and other stakeholders		92		70		143		70		3		70
DOJ employees and stakeholders at Integrity Briefings		3,850		3,000		8,369		3,000		828		3,000

* Indicators for which the OIG only reports actuals.

In FY20 this measure was discontinued. The OIG's caseload has shifted to more complex and document-intensive cases (e.g., grant and contract fraud, leak matters) that require more in-depth financial and foresnsic analysis and document review. The OIG is also diversifying its caseload to extend more investigative coverage to other Deparment components. Therefore, this metric does not accurately reflect work load quality or cases closed.

PERFORMANCE AND RESOURCES TABLE (Goal 1) (continued)												
Decision Unit: OIG/Audits, Inspections, Investigations, and Reviews												
DOJ Strategic Plan: Strategic Objective 4.1: Uphold the rule of law and integrity in the proper administration of justice.												
OIG General Goal #1: Detect and deter misconduct in programs and operations within or financed by the Department.												
WORKLOAD/RESOURCES	**FY2019**		**FY2020**				**FY2021**				**FY2022**	
	Actuals		**Projected**		**Actuals**		**Projected**		**Actuals 1st Qtr**		**Projected**	
Total Costs and FTE	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
(reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total)	442 69	$101,000 [$14,120]	490 27	$105,000 [$14,669]	505 25	$105,000 [$14,669]	466 68	$120,565 [$15,051]	466 68	$120,565 [$15,051]	514 20	$137,184 [$15,255]
Performance Measure												
Intermediate Outcome												
Percentage of BOP Investigations closed or referred for prosecution within 6 months of being opened **[Refined Measure]**		86%		75%		92%		75%		100% (27/27)		*
Number of closed Investigations substantiated*		156		*		157		*		31		*
Arrests *		74		*		89		*		20		*
End Outcome												
Convictions *		64		*		50		*		11		*
Administrative Actions *		179		*		138		*		26		*
Response to Customer Surveys:												
Report completed in a timely manner (%)		100%		90%		98%		90%		100% (14/14)		90%
Issues were sufficiently addressed (%)		100%		90%		100%		90%		100% (14/14)		90%
* Indicators for which the OIG only reports actuals.												

PERFORMANCE AND RESOURCES TABLE (Goal 1) (continued)

Decision Unit/Program: OIG/Audits, Inspections, Investigations, and Reviews

DOJ Strategic Plan: Strategic Objective 4.1: Uphold the rule of law and integrity in the proper administration of justice.

OIG General Goal #1: Detect and deter misconduct in programs and operations within or financed by the Department.

Data Definition, Validation, Verification, and Limitations

A. Data Definition:

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

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

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

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

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

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

C. FY 2020 Performance Report:

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

PERFORMANCE MEASURE TABLE (Goal 1) (continued)									
Decision Unit/Program: OIG/Audits, Inspections, Investigations, and Reviews									
DOJ Strategic Plan: Strategic Objective 4.1: Uphold the rule of law and integrity in the proper administration of justice.									
OIG General Goal #1: Detect and deter misconduct in programs and operations within or financed by the Department.									
Performance Measure Report Workload	**FY2016**	**FY2017**	**FY2018**	**FY2019**	**FY2020**		**FY2021**		**FY2022**
	Actuals	**Actuals**	**Actuals**	**Actuals**	**Projected**	**Actuals**	**Projected**	**Actuals 1st Qtr**	**Projected**
Workload									
Number of Cases Opened per 1,000 DOJ employees:									
Fraud*	0.42	0.55	0.58	0.49	*	0.56	*	0.09	*
Bribery*		0.09	0.13	0.16	*	0.1	*	0.06	*
Rights Violations*	0.14	0.15	0.18	0.15	*	0.10	*	0.00	*
Sexual Crimes*	0.21	0.25	0.25	0.19	*	0.21	*	0.03	*
Official Misconduct*	1.17	1.18	1.04	1.05	*	0.86	*	0.18	*
Theft*	0.11	0.11	0.1	0.05	*	0.06	*	0.01	*
Investigations closed ##	312	308	255	243	N/A	N/A	N/A		N/A
Integrity Briefings and Presentations to DOJ employees and other stakeholders	83	83	90	92	70	82	70	3	70
DOJ employees and stakeholders attending Integrity Briefings	3,799	5,419	4,606	3,850	3,000	4,536	3,000	828	3,000
Intermediate Outcome									
Percentage of BOP Investigations closed or referred for prosecution within 6 months of being opened [Refined Measure]	83%	92%	87%	86%	75	92%	75	100% (27/27)	*
Number of closed Investigations substantiated (QSR Measure)*	196	204	161	156	*	157	*	31	*
Arrests*	91	116	94	74	*	89	*	20	*
End Outcome									
Convictions*	88	84	60	64	*	50	*	11	*
Administrative Actions*	251	219	252	179	*	138	*	26	*
Response to Customer Surveys:									
Report completed in a timely manner (%)	98%	93%	90%	100%	90%	98%	90%	100% (14/14)	90%
Issues were sufficiently addressed (%)	98%	98%	90%	100%	90%	100%	90%	100% (14/14)	90%

In FY20 this measure was discontinued. The OIG's caseload has shifted to more complex and document-intensive cases (e.g., grant and contract fraud, leak matters) that require more in-depth financial and foresnsic analysis and document review. The OIG is also diversifying its caseload to extend more investigative coverage to other Deparment components. Therefore, this metric does not accurately reflect work load quality or cases closed.

* Indicators for which the OIG only reports actuals.

PERFORMANCE AND RESOURCES TABLE (Goal 2)												
Decision Unit: OIG/Audits, Inspections, Investigations, and Reviews												
DOJ Strategic Plan: Strategic Objective 4.1: Uphold the rule of law and integrity in the proper administration of justice.												
OIG General Goal #2: Promote the efficiency and effectiveness of Department programs and operations.												
WORKLOAD/RESOURCES	**FY2019**		**FY2020**				**FY2021**				**FY2022**	
	Actuals		**Projected**		**Actuals**		**Projected**		**Actuals 1st Qtr**		**Projected**	
Total Costs and FTE	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
(reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total)	442 69	$101,000 [$14,120]	490 27	$105,000 [$14,669]	505 25	$105,000 [$14,669]	466 68	$120,565 [$15,051]	466 68	$120,565 [$15,051]	514 20	$137,184 [$15,255]
Performance Measure												
Workload												
Audit and E&I assignments initiated		98		87	Audit Only E&I Only	108 23		87	Audit Only E&I Only	18 0		87
Percent of CSITAO* resources devoted to security reviews of major DOJ information systems		94%		80%		91%		80%	97%			80%
Percent of internal DOJ audit reports that assess component performance measures		73%		30%		72%		40%	50%			40%
Percentage of E&I assignments opened and initiated during the fiscal year devoted to Top Management Challenges		75%		70%		100%		70%		N/A		70%
Percent of direct resources devoted to audit products related to Top Management Challenges, and GAO and JMD-identified High-Risk Areas		96%		85%		94%		85%	95%			85%
Intermediate Outcome												
Audit and E&I assignments completed		114		87	Audit Only E&I Only	103 7		87	Audit only E&I Only	18 5		87
*Computer Security & Information Technology Audit Office												

PERFORMANCE AND RESOURCES TABLE (Goal 2)
(continued)

Decision Unit: OIG/Audits, Inspections, Investigations, and Reviews

DOJ Strategic Plan: Strategic Objective 4.1: Uphold the rule of law and integrity in the proper administration of justice.

OIG General Goal #2: Promote the efficiency and effectiveness of Department programs and operations.

WORKLOAD/RESOURCES	FY2019		FY2020				FY2021				FY2022	
	Actual		Projected		Actual		Projected		Actuals 1st Qtr		Projected	
Total Costs and FTE	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000	FTE	$000
(reimbursable FTE are included, but reimbursable costs are bracketed and not included in the total)	442 69	$101,000 [$14,120]	490 27	$105,000 [$14,669]	505 25	$105,000 [$14,669]	466 68	$120,565 [$15,051]	466 68	$120,565 [$15,051]	514 20	$137,184 [$15,255]
Performance Measure												
Intermediate Outcome												
Percent of Audit resources devoted to reviews of contracts and contract management		12%		8%		8%		5% - 8%		11%		5% - 8%
Components receiving information system audits		10		6		11		6		7		6
Percent of products issued to the Dept. or other Federal entities containing significant findings or information for management decision-making by Audit and E&I		96%		90%	Audit	90/92 100%		90%	Audit	16/16 100%		90%
					E&I	7/7 100%			E&I	5/5 100%		
					Combined	97/99 98%			Combined	100%		
Percent of more complex internal DOJ (E&I) reviews to be provided to the IG as a working draft within an average of 12 months***		40%		35%		71%		35%		80%		35%
Percent of grant, CODIS, equitable sharing, and other external audits to be completed in draft within 8 months		59%		40%		81%		40%		50%		40%
Percent of less complex internal DOJ audits to be provided to the IG as a working draft within 8 months.		100%		N/A		N/A		N/A		N/A		N/A
Percent of internal DOJ audits to be provided to the IG as a working draft within 13 months		90%		50%		92%		50%		100%		50%

*** This measure was refined in FY 2019 to reflect all reviews with a deadline of 12 months.

PERFORMANCE AND RESOURCES TABLE (Goal 2) (continued)

Decision Unit: OIG/Audits, Inspections, Investigations, and Reviews

DOJ Strategic Plan: Strategic Objective 4.1: Uphold the rule of law and integrity in the proper administration of justice.

OIG General Goal #2: Promote the efficiency and effectiveness of Department programs and operations.

Data Definition, Validation, Verification, and Limitations

A. Data Definition:

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

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

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

C. FY 2020 Performance Report: N/A

PERFORMANCE MEASURE TABLE (Goal 2) (continued)									
Decision Unit/Program: OIG/Audits, Inspections, Investigations, and Reviews									
DOJ Strategic Plan: Strategic Objective 4.1: Uphold the rule of law and integrity in the proper administration of justice.									
OIG General Goal #2: Promote the efficiency and effectiveness of Department programs and operations.									
Performance Measure Report	**FY2016**	**FY2017**	**FY2018**	**FY2019**	**FY2020**		**FY2021**		**FY2022**
	Actuals	**Actuals**	**Actuals**	**Actuals**	**Projected**	**Actuals**	**Projected**	**Actuals 1st Qtr**	**Projected**
Workload									
Audit and E&I assignments initiated	109	104	97	98	87	Audit 108 E&I 23	87	Audit 18 E&I 0	87
Percent of CSITAO resources devoted to security reviews of major DOJ information systems	97%	97%	91%	94%	80%	91%	80%	97%	80%
Percent of issued internal DOJ audit reports that assess component performance measures	67%	72%	91%	73%	30%	72%	40%	50%	40%
Percentage of E&I assignments opened and initiated during the fiscal year devoted to Top Management Challenges.	86%	100%	66%	75%	70%	100%	70%	N/A	70%
Percent of direct resources devoted to audit products related to Top Management Challenges, and GAO and JMD-identified High-Risk Areas	95%	92%	88%	96%	85%	94%	85%	95%	85%
Intermediate Outcome									
Audit and E&I Assignments completed	98	112	96	114	87	Audit 10 E&I 7	87	Audit 18 E&I 5	87
Percent of Audit resources devoted to reviews of contracts and contract management	14%	14%	16%	12%	8%	8%	5% - 8%	11%	5% - 8%
Components receiving information system audits	9	10	10	10	6	11	6	7	6
Percent of products issued to the Dept. or other Federal entities containing significant findings or information for management decision-making by Audit and E&I	100%	92%	96%	96%	90%	Audit-E/I 98%	90%	Audit 100% 16/16	90%
Percent of more complex internal DOJ (E&I) reviews to be provided to the IG as a working draft within an average of 12 months ***	N/A	N/A	N/A	40%	35%	71%	35%	80%	35%
Percent of grant, CODIS, equitable sharing, and other external audits to be completed in draft within 8 months	50%	50%	51%	59%	40%	81%	40%	50%	40%
Percent of less complex internal DOJ audits to be provided to the IG as a working draft within 8 months	100%	100%	100%	100%	N/A	N/A	N/A	NA	N/A
Percent of internal DOJ audits to be provided to the IG as a working draft within 13 months	73%	83%	88%	90%	50%	92%	50%	100%	50%

*** This measure will be refined in FY 2019 to reflect all reviews with a deadline of 12 months.

V. Performance, Resources, and Strategies

A. Performance Plan and Report for Outcomes

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

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

B. Strategies to Accomplish Outcomes

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

VI. Program Increases by Item

A. Item Name: Information Technology Division Enhancement				
Strategic Goal(s) & Objective(s):	Uphold the rule of law and integrity in the proper administration of justice			
Organizational Program:	OIG			
Program Increase:	Positions 0	Agt/Atty 0/0	FTE 0	Dollars $0
	Equipment/software/services:			Dollars $2,900,000
Total Request of Increase:	$2,900,000			

1. Description of Item

In an effort for the OIG to continue to promote integrity, efficiency, accountably, and good government through robust independent oversight, the OIG requires a program enhancement of $2.9 million to continue to advance and mature its technology operations. The requested enhancement will support the OIG's continuous effort to create an IT infrastructure that is agile enough to respond to unforeseen events like the COVID-19 pandemic and durable enough to withstand the gradually increasing demand due to the evolving complexity and volume of OIG oversight work. The program enhancement focuses on increasing cloud computing capabilities to consolidate data centers, provide redundancy in the cloud operating environment, safeguard OIG data, and ensure continuity of operations.

2. Justification

A cornerstone of OIG's IT modernization effort has been to shift away from operating data centers and maintaining data center hardware systems to purchasing cloud services. Historically, the OIG requested one-time funding to offset the cost for those IT investments.

In FY 2019, the OIG migrated its core enterprise IT services to the Microsoft Azure Government Cloud environment in support of the Federal Cloud Computing Strategy based on the need to consolidate data centers, provide redundancy in the cloud operating environment, safeguard OIG data, and ensure continuity of operations; however, several physical systems critical to the investigative and analytical functions of the OIG still require migration to the cloud.

Under the old hardware purchase model, in FY 2022, the OIG would be making a multi-million-dollar hardware investment request to sustain its operations by replacing obsolete on-premises equipment. The OIG's current and future use of cloud services shifts us from the hardware investment funding system to one where steady annual funding is required to offset the cost of cloud services. The $2.9 million is designed to fully offset annual IT hardware investments in data center hardware and systems expenses with highly flexible cloud services. This shift to cloud funding was an aspect of OIG's IT modernization strategy that, as noted above, we presented to and for which we received support from OMB.

FY 2020 proved the value of OIG's transition to the cloud over on-premises hardware solutions for its IT services. The portion of the OIG's IT portfolio that was moved to the cloud prior to the COVID pandemic was unaffected by the switch to maximum telework. Support of enterprise IT services did not just continue, but indeed, ITD was able to substantially enhance services over the past 12 months. On the other hand, aspects of our IT portfolio that were not cloud based, such as the OIG's data analytics platform and the technology employed by our Cyber Investigations Office required OIG personnel to maintain hardware systems, often times having to be on site during the pandemic, to do so. Added to this challenge was the recent SolarWinds threat wherein those particular on-premises OIG systems faced greater risk because the operating systems and the hardware itself were much older and less secure than the cloud environment to which other IT systems had been migrated.

The Offices of Cyber Investigations and Data Analytics are seeking to leverage cloud technology to provide secure, remote access to forensic virtual machines, digital evidence, and large data files to replace expensive, standalone, on-premise hardware. This capability will allow for greater collaboration within the OIG with increased use of virtual desktops to support additional OIG investigations and exams. Additionally, in FY 2021, the OIG requested dedicated funding to establish an OIG-wide, enterprise Electronic Discovery (eDiscovery) capability and to replace end of life mission-critical case management systems supporting OIG audits and investigations. Initial funding was approved by OMB in FY 2021 to initiate the case management systems in the cloud, and this enhancement will allow the platforms to run optimally in the cloud; thus, the OIG is required to expand its current cloud presence.

3. Current State and Impact on Performance

Without the enhancements noted above, the OIG will not be optimally positioned to meet rising demands on the IT infrastructure or remain agile enough to respond to future events like the COVID-19 pandemic. Specifically, direct impacts include the OIG's inability to continue hardening the organization's enterprise IT environment against persistent and increasingly complex security threats, expanding its use of physical data centers, and management of IT hardware instead of improving its focus on IT as a service through efficient use of cloud computing resources.

Funding
Information Technology Division (ITD) Enhancement
(Dollars in Thousands)

Base Funding

FY2020 Actual				FY2021 Enacted				FY2022 Current Services			
Pos	Agt/Atty	FTE	$(000)	Pos	Agt/Atty	FTE	$(000)	Pos	Agt/Atty	FTE	$(000)
26	0/0	26	$10,834.0	29	0/0/	29	$15,352.5	29	0/0	29	$11,641.0

Non-Personnel Costs

Non-Personnel Item	FY 2022 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2023 (Net change from 2022)	FY 2024 (Net change from 2023)
Cloud migration	$2,900.0	N/A	1	($1,000.0)	$0.0
Total Non-Personnel	**$2,900.0**	**N/A**	**1**	**($1,000.0)**	**$0.0**

Total Request for this Item

	POS	Agt/Atty	FTE	Personnel ($000)	Non-Personnel ($000)	FY 2022 Total ($000)	FY 2023 Net Annualizations (change from 2022)($000)	FY 2024 Net Annualizations (change from 2023)($000)
Current Services	29	0/0	29	$6,180.7	$5,460.3	$11,641.0	N/A	N/A
Increases	0	0/0	0	$0.0	$2,900.0	$2,900.0	($1,000.0)	$0.0
Grand Total	**29**	**0/0**	**29**	**$6,180.7**	**$8,360.3**	**$14,541.0**	**($1,000.0)**	**$0.0**

B. Item Name: Physical Infrastructure Modifications to Ensure Productivity Post-Pandemic

Strategic Goal(s) & Objective(s):	Uphold the rule of law and integrity in the proper administration of justice			
Organizational Program:	OIG			
Program Increase:	Positions 0	Agt/Atty 0/0	FTE 0	Dollars $0
	Equipment/software/services:			Dollars $2,950,000
Total Request of Increase:	$2,950,000			

1. Description of Item

The COVID-19 pandemic caused the OIG to reevaluate how it organizes and depends upon its physical offices and facilities to fulfill its mission. While the pandemic required immediate action to ensure the safety of OIG employees, the need for impactful oversight of DOJ national security programs did not slow. However, given the OIG's limited options for accessing and storing highly sensitive classified information, the OIG had to postpone critically important national security-related work. Accordingly, the OIG requests $2.95 million to ensure the OIG continues providing high quality oversight of the DOJ's national security programs and operations.

2. Justification

The COVID-19 pandemic has highlighted the need to operate remotely in a geographically distributed manner. In addition, the pandemic has demonstrated that investing in its classified office spaces is critical to ensuring continued OIG oversight of DOJ national security programs. Building SCIFs in targeted field offices will enable OIG field staff to conduct this crucial oversight without the time and expense required to travel to SCIFs in Washington, D.C.

The OIG requests $2.95 million to construct and maintain Sensitive Compartmented Information Facilities (SCIFs) in several OIG field locations. Our initial request specified that our plan is to use this funding to complete the construction over 3 years. Funding for construction of the SCIFs is critical to the OIG's capability to efficiently conduct oversight of the Department's national security work. In view of the fact that protecting national security is among the Department's highest priories, OIG oversight work in this area has been growing, and numerous of our recent reports have demonstrated its value to Department leadership.

Currently, the OIG has only three SCIFs, all of which are located in the Washington metropolitan area. It would not be possible to staff all of our national security work in our headquarters location. Accordingly, OIG national security audits and investigations are also regularly conducted by our field offices. Recent important audits of national security programs have been conducted by our audit offices in Chicago, Denver, Philadelphia, and San Francisco. Other Audit Division and Investigations Division field offices have also conducted audits or investigations involving highly classified material required to be stored or processed in a SCIF. When handling these matters, our field staff have been required to travel to Washington throughout the period their work is pending and are limited in the work they can complete otherwise. This increases our costs to complete these reviews, and as importantly, increases the time for the reviews to be completed. For example, in one audit that involves Top Secret (TS) and Sensitive Compartmented Information (SCI) material, the OIG incurred over $50,000 in travel expenses (plus the non-monetary travel time costs) to enable the OIG's staff from the Philadelphia Audit Office to work on the matter in a SCIF in Washington. Moreover, travel restrictions during the COVID-19 pandemic delayed completion of work on this matter, and has similarly delayed a Chicago audit matter because of the audit teams inability to work on the matters in Philadelphia or Chicago, respectively, and have been restricted from traveling during the pandemic.

In addition, construction of a SCIF at the OIG's Denver field office is important from a continuity of operations perspective. Denver is the OIG's devolution site, and without a SCIF in that office, OIG leadership could be uninformed about developments during a time of crisis, and potentially unable to communicate with Department leadership.

3. Current State and Impact on Performance

Without the requested program enhancement, the OIG will continue to require its field office staff, when necessary, to travel to Washington, D.C., to conduct some of its most highly classified national security work. The additional cost and time required for travel reduces the timeliness of the relevant report, and therefore the potential impact of the OIG's findings. Further, the inability to process highly classified information in OIG field locations has and will increasingly affect the OIG's capacity and decisions to open important oversight audits, reviews, and investigations that involve national security information. Also, as stated above the OIG's Philadelphia COOP site does not have SCIF capabilities, which prevents it from accessing highly classified information, if necessary.

Funding
Physical Infrastructure Modifications to Ensure Productivity Post-Pandemic
(Dollars in Thousands)

Base Funding

FY2020 Actual				FY2021 Enacted				FY 2022 Current Services			
Pos	Agt/Atty	FTE	$(000)	Pos	Agt/Atty	FTE	$(000)	Pos	Agt/Atty	FTE	$(000)
0	0	0	$384.6	0	0	0	$1,884.6	0	0	0	$436.4

Non-Personnel Costs

Non-Personnel Item	FY 2022 Request ($000)	Unit Cost ($000)	Quantity	Annualizations ($000)	
				FY 2023 (Net change from 2022)	FY 2024 (Net change from 2023)
SCIF Construction	$2,950.0	N/A	1	($2,950.0)	$0.0
Total Non-Personnel	**$2,950.0**	**N/A**	**1**	**($2,950.0)**	**$0.0**

Total Request for this Item

	POS	Agt/Atty	FTE	Personnel ($000)	Non-Personnel ($000)	Total ($000)	FY 2023 Net Annualizations (change from 2022)($000)	FY 2024 Net Annualizations (change from 2023)($000)
Current Services	0	0/0	0	$0.0	$436.4	$436.4	N/A	N/A
Increases	0	0/0	0	$0.0	$2,950.0	$2,950.0	($2,950.0)	$0.0
Grand Total	**0**	**0/0**	**0**	**$0.0**	**$3,386.4**	**$3,386.4**	**($2,950.0)**	**$0.0**

VII. Appendix

A. Statistical Highlights

April 1, 2020 – September 30, 2020

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, 2020 - September 30, 2020	
Allegations Received by the Investigations Division	8,820
Investigations Opened	125
Investigations Closed	124
Arrests	32
Indictments/Information	38
Convictions/Pleas	18
Administrative Actions	49
Monetary Recoveries	$ 4,536,390.60
Audit Reports Issued	44
Questioned Costs	$8,456,385
Funds Recommended for Better Use	$1,121,734
Recommendations for Management Improvements	316
Single Audit Act Reports Issued	34
Questioned Costs	$1,854,601
Recommendations for Management Improvements	73
Other Audit Division Reports Issued	6