Council of the
INSPECTORS GENERAL
on INTEGRITY and EFFICIENCY

Top Management and Performance Challenges Facing Multiple Federal Agencies

February 2021

Table of Contents

INTRODUCTION

Each year, Federal Inspectors General (IGs) identify and report on the top management and performance challenges (hereinafter referred to as top challenges) facing their respective agencies pursuant to the Reports Consolidation Act of 2000. This report represents the second time the Council of the Inspectors General on Integrity and Efficiency (CIGIE) has created a summary of the top Federal agency challenges identified by their respective Offices of Inspector General (OIGs).

Approach to This Report

Under the auspices of CIGIE, this report summarizes top challenges that were identified by Federal IGs as part of their recent top challenges reports. In response to a data call from CIGIE, IG offices identified top challenges facing their respective agencies from a list of commonly occurring challenges. IGs could also provide open-ended responses that were not on that list. The resulting top challenges are as follows:

- Information Technology Security and Management (73 percent of respondents)
- Human Capital Management (50 percent)
- Financial Management (48 percent)
- Homeland Security, Disaster Preparedness, and COVID-19 (47 percent)
- Procurement Management (43 percent)
- Grant Management (43 percent)
- Performance Management and Accountability (42 percent)

A group of 15 individuals from across various Federal OIGs drafted this report, with smaller teams assigned to each of the identified top challenges. These mini teams consolidated information from top challenges reports across Federal OIGs to create this report.

A Note About the Coronavirus Disease 2019 (COVID-19)

Several IGs identified the COVID-19 pandemic as a challenge their agencies faced both in the past year and looking forward. In addition, many IGs included COVID-19 when describing other top challenges within their agencies. For example, COVID-19 complicated agencies' efforts to manage finances, complete procurements, or distribute grants. In this report, as appropriate, we discuss COVID-19 as an agency challenge and also describe how COVID-19 affected other agency challenges.

Separately, the Pandemic Response Accountability Committee (PRAC) has created a report summarizing top challenges specific to the COVID-19 pandemic. We have worked with the PRAC to ensure our respective efforts are complementary.

Background on Inspectors General

In accordance with the Inspector General Act of 1978, as amended (IG Act), virtually all Federal agencies have an IG. As of the writing of this document, 75 agencies had an IG; about half of these IGs were presidentially appointed and Senate confirmed, and the other half were appointed by the agency head. The 75 IGs collectively make up CIGIE, which, in addition to creating reports that address matters of mutual concern to IGs, provides training for OIG employees; develops policies, professional standards, best practices, and common approaches for the work of OIGs;

coordinates reviews by OIGs on issues that span multiple agencies; and, through its Integrity Committee, receives, reviews, and refers for investigation allegations of wrongdoing made against IGs, designated staff members of those IGs, and the Special Counsel and Deputy Special Counsel of the Office of Special Counsel.

The role of IGs, according to the IG Act, is to prevent and detect fraud, waste, and abuse and to promote economy, efficiency, and effectiveness within agency programs and operations. IGs are unique in that they have a dual reporting responsibility both to their agency head and to Congress. In this reporting, IGs keep each party fully and currently informed about problems and deficiencies in their agencies' programs and operations and the necessity for and progress of corrective action. To assist with this reporting, IGs have mandatory reporting requirements that include Semiannual Reports to Congress, annual audits of agency financial statements, annual evaluations of information security programs and practices, annual reports on agency improper payments, and annual discussions of the top challenges within their agencies.

To facilitate the reporting of fraud, waste, and abuse to OIGs, each agency's website homepage must contain a direct link to the agency's OIG website. In addition, the IG Act explicitly prohibits government personnel from retaliating against an employee who acts as a whistleblower, and OIGs are responsible for protecting whistleblowers from such retaliation. The IG Act also requires OIGs to report instances of whistleblower retaliation in their Semiannual Reports to Congress.

IGs are nonpartisan and are selected without regard to political affiliation. As such, IGs typically remain in office when presidential administrations change, a practice that has been followed for more than 40 years. In addition, IGs maintain their independence, in both fact and appearance, to provide credible oversight. Agency heads may not prevent IGs from initiating, carrying out, or completing any audit, evaluation, investigation, or special review, except in limited circumstances.

Under the IG Act, IGs are given broad statutory authorities, including access to all agency records and information. Agencies must not prevent IGs from gaining access to records and information necessary to complete any audit, evaluation, investigation, or special review. Efforts on the part of an agency to prevent access to records or information requires IGs to alert Congress and possibly create a 7-day letter. Section 5(d) of the IG Act requires IGs to alert their agency heads of particularly serious or flagrant problems, abuses, or deficiencies, and then the agency head must pass that information, with any comments, to the appropriate committees and subcommittees in Congress within 7 calendar days.

CHALLENGE
Information Technology Security and Management

The information technology (IT) security and management challenge includes top challenges related to the protection of Federal IT systems from intrusion or compromise by external or internal entities and the planning and acquisition of replacing or upgrading IT infrastructure. This is a long-standing, serious, and ubiquitous challenge for Federal agencies because agencies depend on reliable and secure IT systems to perform their mission-critical functions. The security and management of government IT systems remain challenges due to significant impediments faced by Federal agencies, including resource constraints and a shortage of cybersecurity professionals.[1]

Key Areas of Concern

Key areas of concern related to IT security and management include safeguarding sensitive data and information systems, networks, and assets against cyber-attacks and insider threats; modernizing and managing Federal IT systems; ensuring continuity of operations; and recruiting and retaining a highly skilled cybersecurity workforce.

Safeguarding Sensitive Data and Information Systems

Federal information systems continue to be targets of cyber-attacks of increasing complexity. In the face of this ever-present threat, Federal agencies face challenges in ensuring that information systems are secure and sensitive data are protected. Given the immense responsibilities that Federal agencies are charged with, failure to meet this challenge can have significant consequences in a number of ways, including by exposing individuals' personal information and compromising national security. For instance, in December 2020, the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 21-01 regarding the compromise of commercial software used by multiple Federal agencies. CISA's emergency directive stated the exploitation poses an "unacceptable risk to Federal Civilian Executive Branch agencies" based on the compromised products' widespread use to monitor traffic on major Federal network systems, high potential for a compromise of agency information systems, and grave impact of a successful incursion.

The national security impact of cyber-attacks extends beyond Federal information systems into critical public and private infrastructure. The DHS OIG reported that DHS still faces challenges in improving the quality of cyber threat information it shares across Federal and private-sector entities. CISA's lack of progress in improving the quality of information it shares was attributed to a number of factors, such as limited numbers of participants sharing cyber indicators with CISA, delays in receiving cyber threat

[1] U.S. Government Accountability Office, *Financial Audit: Fiscal Years 2016 and 2015 Consolidated Financial Statements of the U.S. Government*, GAO-17-283R (12 January 2017), p. 5.

intelligence standards, and insufficient CISA office staff.

Weak controls over information systems can also result in cyber-attacks and fraud committed against members of the public. The Department of Education (ED) OIG identified a cyber-crime scheme targeting Federal student financial assistance funds. This scheme involved the use of phishing to obtain a student's login credentials and then using this information to access the school's systems to change the student's direct deposit information. The OIG issued a memorandum that informed ED that the lack of two-factor authentication contributed to this incident and recommended that ED take steps to advise schools of this threat.

Some OIGs expressed concern over agencies' progress on improving the maturity of their information security programs. The Department of State (DOS) OIG reported that although DOS has taken steps to improve its information security program, the OIG's annual assessment of the Department's information security program, as in prior years, identified numerous control weaknesses that affected program effectiveness and increased DOS's vulnerability to cyber-attacks and cybersecurity threats. Similarly, the FDIC OIG's annual information security assessment found control weaknesses that limited the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at risk. The AmeriCorps OIG reported that efforts to improve IT security have stagnated, with maturity measures at the second lowest level, unchanged since FY 2017.

In 2020, the Department of Defense (DOD) OIG issued a follow-up report on corrective actions taken by DOD Components in response to cyber vulnerabilities previously identified. The DOD OIG determined that the DOD Components that were reviewed did not consistently mitigate vulnerabilities or include unmitigated vulnerabilities in plans of action and milestones. The U.S. Government Accountability Office (GAO) also reported that DOD has not completed tasks associated with cyber hygiene initiatives dating back to 2015, including some that were supposed to be completed in 2016 and 2018.[2] The Office of Personnel Management (OPM) OIG identified 92 open recommendations from its annual Federal Information Security Management Act and related information systems audits. Several of these recommendations refer to internal control weaknesses identified as far back as 2008.

IT Modernization

Outdated or obsolete IT systems can impede budgeting for long-term IT enhancements, lead to overspending, cause unnecessary IT support efforts, potentially reduce system reliability, and affect an agency's ability to fulfill its mission.

Many OIGs found that their respective agencies were using legacy IT systems to perform core functions and responsibilities. The Department of Housing and Urban Development (HUD) OIG noted that the agency continues to manage most of its operations with outdated legacy systems that cannot be adapted to handle the increasingly complex tasks required to fulfill HUD's mission. In addition, these aging systems are no longer supported by vendors, placing HUD's IT systems at an increased risk of failure and exploitation because critical updates to fix vulnerabilities are often no longer available.

HUD OIG also noted that over the past 5 years, HUD has dedicated a significant amount of its IT budget—between 70 and

[2] U.S. Government Accountability Office, *Cybersecurity: DOD Needs to Take Decisive Actions to Improve Cyber Hygiene*, GAO-20-241 (13 April 2020).

95 percent of its $280 million (on average) annual IT budget—on operations and maintenance. With each successive year since 2012, HUD has continued to spend more on operating and maintaining legacy systems in place of efforts to develop, modernize, and enhance its IT systems. Outdated IT systems can also impact the security of the agency. The DOJ OIG stated that the agency's COVID-19 pandemic response highlighted how some of DOJ's IT services are fragmented or need modernization to perform optimally. DOJ OIG also stated that IT gaps highlight the need for the Department to focus on its enterprise IT capabilities to improve the day-to-day mission capabilities of the Department and better position it to perform during a crisis.

The cost of maintaining legacy IT systems has also inhibited efforts to develop and implement updated IT systems, as agencies are forced to grapple with limited budgets and competing priorities. In particular, the Social Security Administration (SSA) OIG stated that the SSA spent much of its IT funding—$2 billion in FY 2020—on operating and maintaining existing systems. The SSA OIG also stated that SSA has taken an incremental approach to IT modernization by replacing system components rather than whole systems. However, the SSA OIG noted that this approach is no longer viable because technology is advancing faster than SSA can incrementally modernize.

In addition, the failure to improve and modernize IT systems can threaten national security. The DHS OIG found that the slow performance of a critical pre-screening system greatly reduced U.S. Customs and Border Protection officers' ability to identify passengers who may be of concern, and frequent network outages hindered air and marine surveillance operations. The AmeriCorps OIG reported the opposite problem. Its agency was forced to write off as a total loss $37.7 million invested in two unsuccessful efforts to develop a new grants management IT system to replace its outdated legacy structure.

Continuity of Operations

In the event that an IT system is compromised —whether by cyber-attack, environmental anomaly, or some other incident—it is imperative that vital IT systems are available in a timely fashion to support the continuity of operations of Federal agencies. As such, it is critical that agencies prepare for the worst by having a developed-and-tested IT contingency plan in place to ensure that an emergency or crisis will not unduly impact agency programs or operations.

Nevertheless, some OIGs have noted deficiencies with agency IT contingency planning. The HUD OIG reported that concerns and risks associated with HUD's supply chain have not been incorporated into its contingency planning program. Specifically, within the current infrastructure, there are risks associated with the following: alternative suppliers of system components, alternative suppliers of systems and services, denial of service attacks to the supply chain, and planning for alternative processes if critical systems are unavailable. The DOS OIG reported that deficiencies related to developing, testing, and training on contingency plans were found to be persistent in several embassies, which failed to complete or annually test unclassified and classified IT contingency plans. Department standards require management to develop and test IT contingency plans annually for effectiveness and to determine the embassy's readiness to execute them during unplanned system outages or disruptions.

Building and Maintaining an IT Workforce

Many Federal agencies face challenges in attracting and retaining a highly skilled cybersecurity workforce to fulfill mission-critical activities, including modernizing IT

systems and mitigating cyber-attacks. A significant impediment for agencies to expand the Federal cybersecurity workforce is a shortage of available cybersecurity professionals. For example, the DOD OIG noted in its top challenges report for FY 2021 that the congressionally mandated Cyberspace Solarium Commission found that the U.S. Government has a shortage of more than 33,000 cyber personnel.[3] Many agencies also noted that highly skilled personnel are in high demand and that the private sector can offer higher salaries to attract talent. In addition, challenges such as identifying skill sets necessary to address current and emerging threats and an aging workforce have also affected Federal agencies' ability to recruit, train, and retain qualified staff. These challenges are discussed in further detail in the Human Capital Management section of this report.

[3] United States Cyberspace Solarium Commission, *United States Cyberspace Solarium Commission Report* (11 March 2020).

CHALLENGE
Human Capital Management

The human capital management challenge includes top challenges related to recruiting, managing, developing, and optimizing agency human resources. Human capital management remains a significant challenge that affects the ability of Federal agencies to meet their performance goals and execute their missions efficiently. GAO first identified strategic human capital management within the Federal government as a high-risk area in 2001.[4]

Key Areas of Concern

Key areas of concern related to human capital management include recruiting and retaining highly skilled staff, providing adequate training, and leadership continuity.

Recruiting and Retaining Highly Skilled Staff

The inability to attract specialized, highly skilled staff in mission-critical areas of IT, acquisition, healthcare, national security, and intelligence can cause skill gaps that significantly affect Federal agencies' ability to meet their missions. For example, the Department of Commerce (DOC) OIG reported that its acquisition workforce is required to have technical expertise and program management skills to manage a variety of highly specialized products and services, such as large, complex IT systems and scientific and satellite equipment. However, the DOC OIG cited difficulty in attracting experienced acquisition professionals to work in locations outside the Washington, DC metropolitan area and the timeliness of filling vacancies as critical workforce challenges. Similarly, the U.S. Government Publishing Office (GPO) continues to face challenges in filling the mission-critical positions needed to transform the agency from print to digital publishing. As a result, the GPO OIG reported that GPO has several cadre positions in the critical areas of acquisition services, finance, and human capital that remain vacant. The Treasury Department also reported that it has several national security and intelligence positions that, if approved, could create vacancies that are difficult to fill because of the expertise required for these positions.

Several IGs reported that, due to market competition, their agencies faced difficulty in recruiting and retaining highly qualified candidates with the right skills, abilities, and knowledge to fill vacant positions. The Export-Import Bank of the United States (EXIM) OIG recently reported that retaining highly skilled employees was difficult because EXIM must compete not only with the private sector but also with other financial regulatory agencies that compensate employees

[4] GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (6 March 2019), p. 60.

pursuant to pay systems based on the Financial Institutions Reform, Recovery, and Enforcement Act and award higher salaries for commensurate GS levels. EXIM management also expressed concerns that recruitment and retention were more challenging as the private sector reimagined its long-term operations, such as a permanent shift to remote work. The DOJ OIG reported ongoing challenges in recruiting and retaining experienced cyber investigators and attorneys, as these individuals are offered higher salaries in the competitive private sector. DOJ OIG also noted in previous reporting that healthcare and cyber professionals are highly sought in the private sector and often receive salaries that cannot be matched by the Federal pay scale. Similarly, the Defense Intelligence Agency (DIA) OIG reported DIA must develop innovative strategies and take advantage of available employee incentives to ensure the agency can compete with the private sector for acquiring and retaining talent.

Providing Adequate Training

In addition to recruiting and retaining employees, agencies must ensure that staff are adequately trained. The DOS OIG reported that underqualified staff developed deficient performance work statements that led to multiple poorly designed projects and millions of dollars in wasted funds. The DIA OIG noted that sensitive information was placed at risk for unauthorized disclosure because the agency had failed to standardize a training program that ensured that Personnel Security Program employees understood the adjudication policies, processes, and practices for assessing, validating, and certifying applicant eligibility for access to national security information. The DIA OIG also reported that standardizing training could help DIA in identifying, assessing, and mitigating counterintelligence risks to mission-critical acquisitions.

Leadership Continuity

High turnover of leadership positions, a large number of vacant key leadership positions, and an abundance of executive and senior management employees eligible to retire in the next 5 years can affect Federal agencies' ability to meet mission-critical objectives and statutory responsibilities. Specifically, at the Federal Deposit Insurance Corporation (FDIC), 42 percent of current employees (on board as of 1 June 2020) are eligible to retire within the next 5 years. These retirement figures include retirement eligibility of 60 percent of FDIC executives and managers. Although these projections are for a future need and the history at FDIC shows that employees may not retire on their eligibility date, the wave of potential retirements could deplete the FDIC's institutional experience and knowledge, especially during a crisis. Conversely, the Treasury Department had immediate concerns over key leadership positions in its Office of Terrorism and Financial Intelligence (TFI) that have remained vacant. These key leadership positions include the under secretary for TFI, which has been vacant since October 2019, as well as the assistant secretary for terrorist financing, which became vacant in 2020. The National Labor Relations Board (NLRB) OIG noted turnover and vacancies during its audit of the lapse in the FY 2019 appropriation. The NLRB observed that from around April 2018 to January 2019, the chief financial officer (CFO) position was vacant, with a manager designated as acting CFO while also serving in her permanent position. The Office of the CFO was without a permanent budget officer from around January 2019 to April 2019. Vacancies in key leadership positions and retirements could potentially result in leadership gaps and a lack of continuity in operations.

CHALLENGE
Financial Management

The financial management challenge includes challenges related to a broad range of functions, from program planning, budgeting, and execution to accounting, audit, and evaluation. Weaknesses in any of these functional areas limit an agency's ability to ensure that taxpayer funds and agency revenues are being used efficiently and effectively and constitute a significant risk to Federal programs and operations.

Key Areas of Concern

Key areas of concern related to financial management include adequate budgets, financial reporting, and the risk of improper payments, especially as it relates to COVID-19 funding.

Adequate Budgets

Several OIGs list stagnant or declining budgets as a challenge in the upcoming year. For example, the OPM OIG lists a potential shortfall in OPM's budget as one of its top four challenges. This shortfall, which arose from the transfer of the background investigation function to DOD, will harm OPM's ability to fund necessary projects. In addition, the Federal Election Commission (FEC) OIG lists budget as a top challenge because the FEC's budget remained the same despite a dramatic increase in campaign expenditures and the number of transactions subject to FEC regulation. The Amtrak OIG also indicated budgetary concerns, noting that the company went from being on track to post its best financial performance in its 49-year history to experiencing a 97-percent drop in ridership due to the COVID-19 pandemic, placing the company in dire financial straits.

Other OIGs discussed revenue challenges for agencies that rely partially or fully on agency fees and revenues. The GPO OIG identified budget as an issue, noting that the GPO receives only 16 percent of its funding from appropriations. The GPO OIG said the agency needs to better position itself through effective advertising and marketing strategies to generate a new level of visibility. In addition, the U.S. Postal Service OIG identified the Postal Service's financial challenges and business constraints as top challenges. The Postal Service, which is required to be self-sustaining through postal revenues, recorded a net loss of $8.8 billion in FY 2019 and continues to be threatened by the change in consumer and business behavior.

In addition, some OIGs reported that a halt in fee collection during periods of the pandemic has left some agencies in dire conditions. The DOC OIG noted that the U.S. Patent and Trademark Office waived fees for some customers impacted by COVID-19, which created financial difficulties for DOC. In addition, the Nuclear Regulatory Commission (NRC) OIG noted that the Commission deferred fee billing from April through June 2020 to mitigate financial impacts on licensees.

Financial Management

While many OIGs reported improvements in agency reporting, several still list financial reporting as an ongoing challenge. For example, the Railroad Retirement Board (RRB) OIG listed several issues with the RRB's financial reporting, including a lack of reporting on improper payments related to the Railroad Medicare program and material weaknesses with RRB financial reporting, including ineffective controls, an inability to communicate with the National Railroad Retirement Investment Trust's auditors, and social insurance valuation. Independent auditors have declined to issue any opinion on AmeriCorps' financial statements since 2017, with nine material weaknesses persisting from year to year. The corporation has entered into a shared services agreement with the Treasury Department for financial management services to improve performance in this area. In addition, the U.S. Department of Veterans Affairs (VA) OIG reported that, due to the complex and disjointed architecture of the VA's legacy financial management system, it has difficulty meeting the increasingly demanding financial management reporting requirements. In March 2019, the GAO's High-Risk List specifically mentioned in the DOD Financial Management area that DOD financial management staff remain insufficient in number, qualifications, and expertise. Finally, the DHS OIG noted that many key DHS financial systems do not comply with Federal financial management system requirements. As such, the limitations of financial systems' functionality add substantially to DHS's challenges in addressing systemic internal control weaknesses and hinder DHS's ability to ensure proper financial planning payments and appropriate internal controls related to funding for the Coronavirus Aid, Relief, and Economic Security Act (CARES Act).

Risk of Improper Payments

While the COVID-19 pandemic has led to or exacerbated many challenges covered in other sections of this report, it has also negatively impacted financial management. Many OIGs expressed a concern about the risk of improper payments as a result of COVID-19 relief funding. Some OIGs expressed a concern that the pressure to distribute funding in a timely manner has stressed systems and may result in some controls being bypassed.

For example, the VA OIG expressed concern that the pandemic-related funding has worsened existing problems with the lack of internal oversight and poor planning and has resulted in some controls being circumvented to adjust for emergency conditions. In addition, the VA OIG noted that the pandemic has increased the number of bad actors looking to take advantage of the lack of controls. The Department of Transportation (DOT) OIG said the DOT had recently reduced its improper payment rate to under 1 percent but has concerns that the increased workload from COVID-19 payments results in less time being spent on each review, making it more difficult to detect and avoid improper payments. Therefore, it said the DOT should strengthen its procedures to reduce the risk of improper payments.

In addition to pandemic funding, normal operations can result in improper or other questionable payments. The ED OIG noted that the multitude of Federal, State, nonprofit, and private entities involved in student financial assistance programs creates challenges in efforts to address fraud, waste, and abuse. The Department of Interior (DOI) OIG found that the National Parks Service misused donations from philanthropic partners at 26 of 30 parks visited as part of an evaluation. Finally, the DOJ OIG conducted investigations that resulted in two individuals pleading guilty in 2019 to charges related to providing $1 million of adulterated meat to 32 Bureau of Prisons institutions and three companies and two individuals being debarred in August 2020 for 3 years by the DOJ's Debarment Official for knowingly providing adulterated food products in connection with more than $500,000 in contract awards.

CHALLENGE
Homeland Security, Disaster Preparedness, and COVID-19

The homeland security, disaster preparedness, and COVID-19 challenge is a new top challenge related to preventing and disrupting terrorist attacks, protecting against man-made and natural hazards and disasters, and responding to and recovering from incidents that occur. This new challenge reflects the evolving environment affecting the United States and Federal agencies charged with executing missions related to homeland security and disaster preparedness and recovery. In 2020, the worldwide outbreak of COVID-19 placed significant strain on Federal agencies, and the pandemic continues to challenge their efforts to maintain operations while protecting the health and safety of the Federal workforce and the American public.

Key Areas of Concern

Key areas of concern related to homeland security, disaster preparedness, and COVID-19 include countering terrorism and defending the homeland against security threats, protecting and promoting U.S. technological dominance and economic competitiveness, and maintaining continuity of operations during a global pandemic.

Countering Terrorism and Homeland Security Threats

Protecting the nation's critical infrastructure and deterring adversaries, competitors, and terrorists require Federal agencies to coordinate efforts to manage risks. According to DHS OIG, DHS continues to be challenged to properly plan and provide adequate guidance, oversight, and monitoring of programs and operations to counter terrorism and homeland security threats. For example, a secure and resilient electoral process is a vital national interest and one of the agency's highest priorities. Although DHS improved coordination efforts to secure the nation's systems used for voting, it should take additional steps to protect the broader election infrastructure, which includes polling and voting locations, election technologies, and related storage facilities. The agency also needs to mitigate risks associated with physical security, terrorism threats, and targeted violence to the election infrastructure, and to identify dependencies on external stakeholders that impede mission performance. On Election Day, DHS officials stated that there was no evidence of a major cyber-attack on the elections and that it would continue to monitor hacking attempts and cyber intrusions and coordinate information sharing with State and local officials.

Among agencies' highest priorities are countering threats posed by foreign and domestic terrorism. DOJ OIG states that domestically the United States faces threats by both homegrown violent extremists (HVEs) and domestic violent extremists (DVEs). According to a DOJ OIG report, the Federal Bureau of Investigation (FBI) has not taken sufficient action to resolve certain

weaknesses in its process for assessing potential HVEs and lacks comprehensive strategies to mitigate emerging challenges related to assessing potential HVEs. The FBI has recognized publicly that it believes HVEs and DVEs currently present the greatest terrorist threat to the United States. Furthermore, General Services Administration (GSA) OIG findings related to safeguarding Federal facilities and providing secure work environments demonstrate an ongoing need for GSA's attention in these areas, as Federal buildings have faced a range of security threats during the recent unrest in many cities throughout the country, with some buildings becoming targets for violence and property damage. The Mark O. Hatfield Federal Building in Portland OR has been a frequent focal point of violent protests since the killing of George Floyd.

Combating terrorism, whether on the battlefield or through anti-money-laundering and combating terrorist financing operations, remains critical to addressing this challenge. According to the DOD OIG, DOD will also be challenged to ensure that it maintains sufficient capacity and capability to counter and defeat persistent threats from violent extremist organizations around the world. As DOD has incrementally reduced the personnel and resources that it has deployed for counterterrorism missions around the world over the last several years and has shifted to address the reemergence of nation-state actors, DOD will need to prioritize its counterterrorism objectives by leveraging interagency and international partners effectively, establishing clear priorities, and maximizing investments. Depriving terrorist organizations of financing is critical to defending the homeland. Additionally, Treasure OIG noted that the ability of the Treasury Department's TFI to effectively coordinate, collaborate, and gather and analyze intelligence information requires a stable cadre of experienced staff.

Protecting and Promoting U.S. Technological Dominance and Economic Competitiveness

The United States must develop new concepts and capabilities to protect the homeland, maintain and advance economic prosperity, and effectively lead as a global superpower. The evolving security environment, dominated by the rise of China and Russia and the persistent threat of Iran and North Korea, is challenging how Federal agencies perceive security threats. The National Security Strategy of 2017 stated, "China and Russia challenge American power, influence, and interests, attempting to erode American security and prosperity" through growing political, economic, and military competitiveness.[5]

Promoting the development of new and emerging technologies is critical for the U.S. Government, American industries, and the American people. Emerging technologies, such as artificial intelligence (AI), machine learning, and fifth generation (5G) technologies, have the potential to revolutionize how information is collected and analyzed, while also exposing the same information to manipulation or exploitation by malicious nation-state or nongovernmental actors. According to the DOD OIG, DOD must be more agile and rapidly develop, secure, and deploy new and innovative technologies to secure the competitive advantage and counter similar technology. DOD must also ensure that it is balancing the need to leverage this new technology with identifying and evaluating any ethical risks or unintended consequences resulting from its use. The Intelligence Community OIGs also recognized

[5] National Security Strategy of the United States of America, December 2017, (https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf), p. 2.

the transformative powers of technologies and identified managing AI as an emerging challenge, especially as Federal agencies explore the use of AI to improve processes. Maintaining an economic advantage is also critical to homeland security. Agencies such as DOC that are challenged with helping U.S. companies be more competitive abroad while also protecting U.S. national security interests must continue to evaluate and improve processes for quickly adjudicating company requests. According to the DOC OIG, DOC must strengthen confidence in intellectual property rights by improving the process and must ensure that remedies against imports that threaten national security are evaluated in a transparent, timely manner that does not adversely affect American businesses. According to the Treasury Department OIG, the Treasury's Office of International Affairs expects an increase in its foreign investment transaction reviews due to the expanding jurisdiction of the Committee on Foreign Investment in the United States, and is aggressively hiring staff and implemented a new Case Management System to meet the increasing workload. Maintaining the United States' competitiveness in the global marketplace and its leadership position on the global stage and protecting American technological advances are critical high-risk challenges facing Federal agencies.

Preparing and Responding to Disasters

Changing climate patterns, extreme weather events, and global pandemics have long-term impacts on agencies' personnel and their ability to execute their missions, and the economy. The COVID-19 pandemic further impacts agencies that have significant involvement in addressing other national disasters. For example, the DOI OIG noted that DOI subagencies deploy firefighters every year to support wildfire response, which requires significant collaboration across a wide range of Federal agencies, States, tribes, local land managers, and other stakeholders. Fire camps can include a large number of personnel living together and working collectively to respond to a wildfire, which heightens the risk of exposure to COVID-19.

These disaster-related conditions also have a significant impact on military readiness and infrastructure. Mitigating the impacts of changing climate patterns and extreme weather events on personnel readiness and military infrastructure requires DOD to consider issues during facility design and investment decisions and helps to build resiliency among DOD personnel and on installations, ultimately ensuring continuity in the wake of disasters.

Consequently, revisions to agencies' workforce planning models have also become a priority to help strategically allocate and align agency staff and resources with mission and critical priorities, and for safe reintegration in the COVID-19 environment. Agencies with an international presence, such as the U.S. Agency for International Development (USAID), must also develop plans and procedures to guide the reentry of their domestic and overseas workforce as pandemic conditions allow.

In March 2020, the Peace Corps responded to the COVID-19 pandemic by suspending all volunteer activities and evacuating nearly 6,900 volunteers from about 60 countries of service. For the first time in its nearly 60-year history, the Peace Corps does not have a single active volunteer. The agency faces the tremendous challenge of planning for the resumption of its overseas volunteer programs in the environment of uncertainty that the COVID-19 pandemic has created. While lack of volunteers in the field minimizes previously identified challenges to volunteer health and safety, these unresolved challenges may become more complex as the Peace Corps begins to redeploy volunteers amid the pandemic and as new challenges arise.

Maintaining Continuity of Operations During a Global Pandemic

The CARES Act was signed into law on 27 March 2020 as a result of the COVID-19 pandemic. The CARES Act provided many agencies grant funding to ensure the continuity of operations; fund State, local, and tribal efforts to prevent, prepare for, and respond to COVID-19; and combat COVID-19-related fraud, scams, and violations of Federal antitrust and other laws. Consequently, the additional responsibilities resulting from the CARES Act pose new challenges for Federal agencies, as they must effectively oversee and monitor new grant programs and take additional proactive steps to create and sustain a culture of fraud prevention and awareness and appropriately distribute CARES Act funding, while also continuing to execute their normal agency missions.

Responding to the rapidly evolving COVID-19 pandemic has presented immediate and significant challenges for Federal agencies, most notably in their responsibility to keep their staff, contractors, visitors, and workspaces as safe as possible while also overcoming internal and external technological challenges. Many agencies have taken steps to ensure the continuity of government operations by allowing maximum work-life flexibilities, such as 100-percent telework, unrestricted work schedules, and other employee assistance programs. Even with these flexibilities, many agencies reported increased pressure on employees caused by issues outside of the workplace, which created challenges in maintaining operations and mission success. Many agencies faced internal and external technological challenges, including IT connectivity, which has impacted employee productivity. As many agencies pivoted to large-scale work-from-home operations, the increase in remote access to IT systems also increased the risk of security breaches.

As mass telework continues, agencies are overcoming some of these challenges, but their pandemic response has highlighted how some of the agencies' IT services are fragmented or need modernization to perform optimally. IT challenges are discussed in further detail in the Information Technology and Security Management section of this report.

Agencies that require employees to be physically present to fulfill their duties, given the nature of their work, have faced heightened risk of exposure to COVID-19. Many Federal agencies and personnel expressed concerns with the availability of staff, as well as personal protective equipment (PPE), if there were an outbreak of COVID-19 in their facility. This is especially true for agencies such as DHS and DOJ, which must be concerned not only with possible staff exposure to COVID-19 but also with preventing the spread of the virus among individuals detained in their custody. For example, the pandemic amplified pre-existing medical and correctional staffing shortages at the Federal Bureau of Prisons, which negatively affected some institutions ability to timely and thoroughly respond to COVID-19 and implement strategies to mitigate the impact of the pandemic on inmates and staff.

Many agencies also face challenges to ensure stability and full and effective functioning of its components during COVID-19. For example, DHS recently faced the prospect of furloughing almost 70 percent of its U.S. Citizenship and Immigration Services workforce reportedly due to decreased revenues related to COVID-19. A return to normal operating procedures requires congressional intervention to sustain the agency through FY 2021. Pandemics such as COVID-19 also negatively impact the combat readiness of DOD forces by limiting travel and large-scale exercises, while also stressing supply chains and challenging DOD's ability to maintain the readiness of its stockpiles and

protect the health, safety, and security of DOD personnel and their families. Law enforcement agencies, such as those in DOJ, face increased demands in identifying and prosecuting opportunists attempting to exploit COVID-19 pandemic funding through frauds and other scams that harm the public, while continuing to combat their non-COVID-related responsibilities.

CHALLENGE
Procurement Management

The procurement management challenge encompasses the entire procurement process, including contract award and post-award contract administration.[6] Given that the Federal government awarded more than $586 billion in contracts in FY 2019, approximately 40 percent of its total discretionary budget,[7] the challenges that agencies face in procurement management put billions of taxpayer dollars at increased risk of fraud, waste, abuse, and mismanagement. Moreover, because many Federal agencies rely strongly on contractors to perform their missions, the failure of an agency to properly manage its procurement functions could also impede the agency's ability to execute its mission.

Key Areas of Concern

Key areas of concern related to procurement management include weaknesses with the contract award process, managing and overseeing contractor performance, reviewing invoices and payments, and training and retaining procurement personnel.

Contract Award Process

Several OIGs identified problems related to the contract award process, such as having sufficient controls in place to prevent fraud, estimating costs inappropriately or ineffectively, and mismanaging the competitive bidding process. The GSA OIG, for example, noted that the agency failed to update its suspension and debarment listing. When this occurs, Federal agencies can unknowingly execute contract actions, including new contract awards, with contractors who have been suspended or debarred. The GSA OIG also found several instances where excluded contractors were incorrectly listed on GSA's eTools[8] and one instance where an agency purchased services off a GSA Multiple Award Schedule contract from an excluded contractor. The DOT OIG uncovered challenges in correctly developing independent cost estimates, conducting price and cost analyses, and requiring adequate justification for single bids. After assessing the Federal Aviation Administration's (FAA's) competitive award practices for major acquisition program contracts, the DOT OIG recommended that the FAA could put up to $4.9 billion in Federal funds to better use by improving its ability to establish fair,

[6] Although some Federal agencies define the term "procurement" narrowly as the act of buying goods and services for the government and use the term "acquisitions" to refer to the broader concept of the initiation, design, development, test, contracting, production, and deployment of systems, supplies, or services to satisfy government needs, we use the terms interchangeably for the purposes of this report.

[7] This information comes from GAO. It does not reflect the likely significant increase in contract spending as a result of COVID-19 spending in 2020. The contract spending increase over FY 2018 is approximately 5.8 percent and $132 billion more than contract spending in 2015.

[8] GSA's electronic tools (eTools) help manage an agency's GSA procurement transactions, place orders, or learn about business opportunities.

reasonable, and realistic contract pricing. Other OIGs identified challenges in drafting adequate performance work statements due to a lack of technical knowledge on the part of contracting officer representatives and other procurement personnel. For example, the DOS OIG reported that poorly drafted performance work statements for several overseas construction projects resulted in major structural deficiencies, which required millions of dollars in repairs.

Insufficient award management also creates opportunities for fraud. While agencies take steps to curb fraud, waste, and abuse, the COVID-19 pandemic has created novel opportunities for bad actors, particularly because of the need to facilitate rapid purchases of essential goods and services. For example, the VA OIG found that the VA has struggled to expand its supply chain fast enough to curtail the spread of COVID-19, and many companies have sought contracts for PPE and other medical supplies worth millions of dollars that they cannot actually fulfill. VA OIG investigators collaborating with other law enforcement authorities arrested a Georgia resident for attempting to sell millions of nonexistent respirator masks and other PPE totaling more than $750 million to the VA in exchange for large up-front payments. A USAID OIG investigation exposed fraud and conflicts of interest affecting a $4.7-million USAID-funded agriculture program in Uganda. The USAID OIG's investigation uncovered a conflict of interest involving consultancy contracts, as well as evidence that the project accountant falsified records to substantiate payments.

Contract Oversight

In addition to the contract award process, Federal agencies also face challenges in maintaining robust oversight of contract portfolios and contract execution and performance. The FDIC OIG reported that the FDIC Board and management were challenged to oversee contracts on a portfolio basis because a contracting system did not readily gather, analyze, and report portfolio-wide contract information.

Oversight is also required to determine if applicable laws and regulations are being followed and if the contractor is complying with contract requirements. Critically important to the oversight process is the need to adequately document contractor performance to properly support award fee determinations and suitability of the contractor for future contract award. OIGs identified challenges with monitoring, assessing, and documenting contractor performance, as well as compliance with the Federal Acquisition Regulation (FAR). The DOC OIG, for example, found that inadequate controls and an ineffective process for detecting and following up on contract performance deficiencies have led to procurement officials not complying with the FAR. In an audit of DOJ contracts awarded from FY 2013 through FY 2019, a time in which DOJ awarded more than $54 billion in contracts, the DOJ OIG found frequent noncompliance with the FAR due to inadequate execution of contract oversight responsibilities, insufficient quality assurance practices, and failure to maintain documentation to support procurements. Further, the ED OIG found that ED did not track all identified instances of loan servicer noncompliance and rarely held loan servicers accountable for noncompliance with requirements. The ED OIG also noted that information ED collected was not always sufficient to ensure that loan servicers complied with requirements for servicing federally held student loans.

OIGs also reported challenges with the award fee process. Award fees are provided to the contractor based on a judgmental evaluation by the government, sufficient to provide motivation for excellence in contract performance. The Pension Benefit Guaranty Corporation (PBGC) OIG, for instance, found that procurement personnel had not appropriately designed performance metrics

for key factors required for an aggregate measure of contractor performance. In addition, the PBGC OIG found that procurement personnel awarded the contractor the award fee after considering only one of the three factors (cost, schedule, and performance) that the FAR requires. As a result, the OIG's audit concluded that the $5.1 million award fee payment was unsupported. Similarly, the National Aeronautics and Space Administration (NASA) OIG found that, for a significant number of years, NASA used unclear, outdated criteria to determine award fees, which resulted in paying one of its prime contractors $863 million—which amounted to 91.4% of its available award fees over the period in question—despite significant performance shortfalls, as well as substantial cost and schedule growth. Weaknesses identified by OIGs within contract oversight continue to hinder the Federal government's ability to ensure that goods and services were received within contract terms and in accordance within Federal laws and regulations.

Invoice and Payment Review

OIGs have continued to report instances where agencies fail to appropriately review invoices and track associated payments to ensure that the government received the goods and services for which it had contracted and paid. OIGs reported challenges within several areas of the invoice and payment review process, including a lack of thorough invoice review, inadequate documentation to support payments, and a failure to track expenditures in detail. For example, a DOS OIG report evaluating invoicing practices for four task orders totaling more than $151 million found limited supporting documentation for the selected invoices. The OIG could not verify that all reviewed invoices were processed properly because procurement personnel for three of the four task orders did not maintain records of their invoice reviews. Additional work by the DOS OIG revealed that procurement personnel did not verify that invoiced prices complied with contract terms, resulting in $3.4 million in questioned costs. Internal controls such as these are used to provide reasonable assurance that objectives are met and related risks are mitigated. The ability to determine whether knowledgeable procurement personnel complete the appropriate verifications aids in reducing the likelihood of ensuring only appropriate costs are paid. However, establishing the ability to monitor invoice and payment data requires advanced planning. For instance, the NASA OIG reported that due to the co-mingling of key development activities, NASA had difficulty separating and tracking individual expenditures. Similarly, the FDIC OIG found that the agency did not capture the necessary data to properly track invoices and payments. These deficiencies heighten the risk of fraud, waste, and abuse and also may hinder the ability of an agency to complete its mission as finite resources may be lost to mismanagement.

Training and Retaining Procurement Personnel

The effectiveness of the procurement process depends on retaining and developing a competent workforce that can handle complex acquisitions. The OIGs for the FDIC, GSA, DOC, HUD, DOJ, and DOS found that some Federal contracting officers and other procurement personnel lacked sufficient training in procurement regulations, resulting in problems we have described earlier within this section. Further, some agencies found difficulty in keeping personnel trained and certified in crucial procurement and technical skills necessary for high-value and complex procurements. The DOS OIG found that nearly 50 percent of its reports issued from FY 2017 through FY 2019 that reported inadequate contract oversight cited issues with the training and experience of procurement personnel. The DOC OIG found that it is an ongoing challenge to hire and retain

procurement personnel with the needed skill sets, especially given the high attrition rate and the heavy workload for such personnel. The HUD OIG likewise reported that hiring additional procurement personnel remains a challenge for HUD due to high attrition rates, the heavy workload, and budget constraints.

Without highly skilled procurement personnel, the Federal government will continue to experience significant challenges in procurement planning, oversight, and administration of government contracts sufficient to ensure contractual and legal compliance.

CHALLENGE
Grant Management

The grant management challenge encompasses the entire grant-making process and includes agencies' oversight of awards as well as recipients' internal controls and reporting. Deficiencies in these areas can lead to misspent funds, improper payments, and ineffective programs. Federal agencies spent more than $939 billion through grants in FY 2020—an increase of more than $200 billion relative to FY 2019. This increase is largely attributable to funding from the CARES Act, which dramatically increased the number and size of pandemic relief grant programs for which many agencies are responsible, often with limited to no staffing increases. These factors have created a complex landscape of grant programs for grantees to understand and for agencies to implement, oversee, and evaluate.

Key Areas of Concern

Key areas of concern related to grant management include ensuring funds are awarded properly, overseeing the use of grant funds, ensuring grant investments achieve intended results, obtaining timely and accurate financial and performance information, and threats posed by foreign government talent recruitment programs.

Ensuring Funds Are Awarded Properly

Given the breadth and scope of grant programs, agencies face the challenge of ensuring that agency staff are aware of and abide by all relevant rules in awarding funds. As discussed in the Human Capital Management section of this report, agencies need to recruit, train, and retain an adequate number of qualified staff to properly administer and oversee grants to prevent funds from being awarded to improper recipients or for unintended purposes. It is important for agencies to follow appropriate processes and maintain sufficient documentation so that the agency and the public can determine why an award was made. The lack of such processes and documentation prevents an agency from being able to demonstrate that grants are being awarded to further program goals and could frustrate attempts to recoup improper or fraudulent grant awards.

New programs created under CARES Act authorities have exacerbated this challenge and stretched already strained staff due to a significant influx of grant funds and accelerated award timetables. The DOC, for example, received more than $1.9 billion through the CARES Act to aid communities affected by the pandemic. This amount is close to the entire amount that DOC awarded in grants in FY 2019—$2.2 billion. As the DOC OIG reported, the need to ensure that these funds are distributed promptly, fairly, and for authorized purposes will place increased demands on DOC's workforce, oversight processes, business practices, and financial management systems. The awarding of pandemic relief, contracts, and grants efficiently, effectively, and for intended purposes is also a top challenge that the DOT OIG identified. The OIG pointed to previous

reviews, which identified issues with the qualifications and training of DOT staff who awarded funds and the recipient staff.

Overseeing the Use of Grant Funds

Recipients must use grant funds only for the specific purposes intended in the grant award and must adhere to parameters and guidelines established by law and regulation. Due to the large number of grants, agencies face challenges in developing and maintaining robust grant management systems that can provide the level of oversight needed to ensure grantees use funds solely for authorized purposes. Many agencies, and their recipients, also face challenges in maintaining adequate documentation. Moreover, with the COVID-19 pandemic, agencies face the challenge of developing means to effectively oversee grants when many agency employees, grant recipients, and sub-awardees are working remotely.

The Department of Health and Human Services (HHS) is the largest grant-making agency in the Federal government, awarding about $244.7 billion in FY 2020 (excluding the Centers for Medicare & Medicaid Services). The HHS OIG emphasized that ensuring the transparency and accountability of HHS funds is critical to making sure HHS beneficiaries and the American public get the true benefit of the agency's substantial financial investment. The CARES Act expanded HHS's grant programs to support to the country's COVID-19 response, including vaccine development, clinical trials, and distribution. Without adequate internal controls in place, grant funds may be misspent, duplicate services may occur, and sub-recipients may lack adequate monitoring. Further, insufficient oversight of grant programs poses the risk of significant improper payments. The NASA OIG found that when NASA and its recipients lack adequate systems of internal controls to ensure proper administration and management of awards, it can result in funds not being used for their intended purposes. In a positive development, the AmeriCorps OIG noted that AmeriCorps has made significant progress in developing and implementing a detailed grant risk model to guide all phases of grants management, a longstanding OIG recommendation.

Ensuring Grant Investments Achieve Intended Results

Assessing which grant programs achieve their goals and objectives is an ongoing challenge for Federal agencies and Congress in determining how to spend limited resources. Agencies must continue to meet the challenge of establishing outcome-focused measures for their grant programs. As discussed in the Performance Management and Accountability section of this report, agencies must ensure that objective performance measurement requirements are incorporated into grant agreements. When such measures are not included or are not clearly defined, the government faces an increased risk that money may be wasted or that grants programs are not achieving their intended results.

For example, a DOS OIG review determined that the Global Engagement Center's (GEC's) monitoring and evaluation plans did not include all the monitoring and evaluation elements required by the award program and did not have a direct connection to the proposed scope of work. Accordingly, GEC was not in a position to ensure that recipients were using the funds as intended and could not demonstrate that the awards were fulfilling GEC's statutory mandate.

Obtaining Timely and Accurate Financial and Performance Information

Without accurate, timely, and complete financial and performance data from grantees, agencies cannot determine if funds were spent properly or achieved the intended

results. As discussed in the Financial Management and Performance Management and Accountability sections of this report, when such data are inaccurate, delayed, or incomplete, agencies face increased risk of improper payments and wasted funds. Addressing this challenge, the ED OIG has highlighted the importance of taking steps to ensure strong data management practices across the Department, grantees, and subrecipients. The ED OIG has emphasized the need for continuous outreach to grantees to reinforce program requirements and expectations around good data. This outreach is particularly important regarding new programs related to the COVID-19 pandemic and disaster relief, where ED faces the challenge of collecting, analyzing, and reporting data for many different purposes, such as evaluating programmatic performance, assessing financial compliance, and informing management decisions. The Small Business Administration (SBA) OIG reported that inaccuracies and incomplete financial and performance reporting inhibit policymakers' and the public's ability to track Federal spending effectively, thereby inhibiting effective oversight. The SBA OIG also noted that data inaccuracies negatively affect the agency's ability to report complete and accurate information on time, as required by the Digital Accountability and Transparency Act of 2014.

Threats Posed by Foreign Government Talent Recruitment Programs

Many agencies fund grants to support cutting-edge scientific research and development. The enacted FY 2020 Federal budget, for example, included more than $155.9 billion designated for research and development. The intellectual property generated from this research has economic and scientific value that foreign governments have attempted to acquire through talent recruitment programs. These programs target scientists, engineers, academics, researchers, and entrepreneurs in the United States and offer rewards and attractive opportunities at foreign research institutions in exchange for transferring their knowledge and expertise to foreign countries. Contracts under these programs often include provisions prohibiting disclosure of these agreements, which puts them directly at odds with grant application disclosure requirements that are critical to maintaining the integrity of grant programs and proper oversight. Undisclosed involvement in these programs threatens the integrity of agencies' grant programs and raises concerns regarding national security, conflicts of interest, conflicts of commitment, and intellectual property theft.

The Department of Energy (DOE) OIG, for example, identified theft of research and intellectual property funded by DOE as a top challenge, given DOE's prominent role in advanced research and development across multiple scientific disciplines, as well as its key role in nuclear weapons development. The National Science Foundation (NSF) OIG also identified challenges related to foreign government talent recruitment programs trying to exploit the openness of American universities and threatening the integrity of U.S. research initiatives. While NSF took measures to strengthen its policies and procedures regarding disclosure of foreign involvement in NSF-funded research, NSF and other agencies that fund scientific research, as well as grant recipients, need to continue to assess and refine their controls in this area, to include providing adequate staffing and strengthening certifications and communications with grantees during the life cycle of awards.

CHALLENGE
Performance Management and Accountability

The performance management and accountability challenge includes challenges related to managing agency programs and operations efficiently and effectively to accomplish mission-related goals. Although Federal agencies vary greatly in size and mission, they face some common challenges in improving performance in agency programs and operations.

Key Areas of Concern

Key areas of concern related to performance management and accountability include operational leadership and management challenges, internal control deficiencies, enterprise risk management, working with external stakeholders, and collecting and using performance-based metrics.

Operational Leadership and Management Challenges

Mitigating operational leadership and management challenges is critical to ensuring that an agency can successfully focus on its mission objectives. The DOT OIG identified improving the FAA's oversight of aircraft certification processes and enhancing aviation safety oversight while working in a collaborative environment as top DOT challenges. The Treasury Inspector General for Tax Administration (TIGTA) reported that legislative developments related to tax reform and tax policy present challenges for the Internal Revenue Service (IRS). Implementation of the various tax provisions will result in reprogramming of systems, and changes to tax forms, instructions, and publications. The IRS must also balance tax compliance activities with its efforts to protect taxpayer rights. In addition, TIGTA remains concerned about the IRS's inability to significantly reduce improper payments related to several tax credits. As records management is a core program function for the National Archives and Records Administration (NARA), the NARA OIG identified its need to preserve records and improve records management as top challenges. The AbilityOne OIG reported that the allocation of roles, responsibilities, and resources among the Commission senior staff creates challenges in management's ability to timely implement policies and initiatives, effectively execute changes in the program, and support program growth.The SBA OIG reported that SBA's management and monitoring of the 8(a) Business Development Program needs improvement to ensure that it is providing effective business development assistance to 8(a) firms and that only eligible firms are admitted into and remain in the program. Finally, Amtrak OIG reported that transforming the company in response to the COVID-19 pandemic will challenge the Executive Leadership Team members to collaborate effectively on decisions that benefit the company as a whole. At the same time, leadership must commit to addressing several longstanding, costly management challenges, given both the company's economic distress and its dependence on significant Federal funding.

Another challenge for several agencies was managing large projects or multiple projects simultaneously. The Architect of the Capitol (AOC) OIG reported that managing concurrent

construction projects continues to be a top challenge for the AOC. In addition, due to the lack of a centralized working capital fund, the AOC faces many operational redundancies at the jurisdiction level for large construction projects and other programs that cross multiple funding streams. The NASA OIG reported that NASA's major projects have historically cost significantly more and taken much longer to complete than originally planned, which can affect funding and schedules for other NASA projects.

Agencies also share the challenge of effectively managing records. The AOC OIG also noted that the AOC lacks a sound records management and retention policy. Similarly, the Denali Commission OIG and the Federal Labor Relations Authority OIG each reported that their relative agencies need to establish a complete oversight or governance process for documenting agency policies, procedures, and processes that address the proper handling of all hardcopy and electronic records.

Internal Control Deficiencies

A strong internal control system provides stakeholders with reasonable assurance that operations are effective and efficient and that an agency uses reliable information for decision-making and is compliant with applicable laws and regulations. The Consumer Product Safety Commission (CPSC) OIG reported serious issues related to internal control deficiencies in a number of programs that call into question the accuracy of some of the statements of assurance. The Environmental Protection Agency (EPA) OIG reported that it cannot be certain the EPA has proper procedures in place to address risks and develop plans to mitigate and protect operations from fraud, waste, abuse, and mismanagement, noting that the agency was not conducting risk assessments for 20 programs that collectively cost more than $5.7 billion in FY 2018.

Similarly, the U.S. Department of Agriculture (USDA) OIG noted that fraud, waste, and abuse are critical concerns for the Food and Nutrition Service (FNS). The USDA OIG reported that the FNS needs to improve its oversight and quality control processes for the FNS's Supplemental Nutrition Assistance Program, considering the size and importance of the program, which in FY 2018 served an average of 39.7 million people each month for a total annual cost of $64.9 billion. Moreover, strong oversight controls of a large nutrition assistance program become even more crucial when FNS responds to natural disasters. The USDA OIG also reported that in September 2017, Hurricane Irma and Hurricane Maria devastated Puerto Rico, and although Congress granted $1.27 billion in supplemental nutrition assistance funding, FNS and the Administration for Socioeconomic Development of the Family were not able to distribute essential disaster nutrition grant funding to survivors until 6 months after the hurricanes because Puerto Rico did not have the authority and was unable to operate a disaster nutrition assistance program.

Promoting accountability through careful internal coordination with clear, well-defined lines of authority is an ongoing challenge for DOS. The EPA OIG reported that the EPA lacks a systematic process for regularly assessing the need for policy and procedure updates, which may lead managers to implement individual interpretations of Federal guidance and policies, thereby creating inefficiencies and increasing the opportunity for fraud, waste, abuse, or mismanagement. Similarly, the U.S. International Trade Commission (ITC) OIG reported that the absence of standard procedures results in inconsistencies in how routine operations are performed, reduces the quality of information produced, increases the risk associated with informal decisions made by management overrides, and often results in a lack of documentation to support decisions. In addition, the ITC OIG stated that managers need to remain mindful on how the changing conditions resulting from the COVID-19 pandemic may impact the effectiveness of key internal controls in their processes.

Enterprise Risk Management

An effective enterprise risk management (ERM) approach is necessary for Federal managers to identify, prioritize, and mitigate the impact of uncertainty on an agency's overall strategic goals and objectives. The AbilityOne OIG reported that the Commission has failed to establish a ERM program and that management has made virtually no progress in addressing the lack of ERM, which, according to the OIG, leaves Commission management unable to effectively prioritize and manage risks. The NARA OIG reported that NARA management has not made ERM a strategic priority and has not yet implemented an effective ERM program. The CPSC OIG also reported challenges with its ERM program, noting that it is unclear if the agency's program is sufficiently mature to be auditable. The SBA OIG reported that SBA risk management and oversight practices need improvement to ensure the integrity of loan programs. In FY 2020, SBA did not always conduct planned high-risk lender reviews, recommend appropriate and consistent risk mitigation actions for the deficiencies identified during the oversight reviews of high-risk lenders, or communicate loan deficiencies noted during high-risk lender reviews to SBA approval and purchase loan centers. In addition, over the course of a decade, the SBA OIG investigated at least 22 cases with confirmed loan agent fraud totaling about $335 million.

As a result of the COVID-19 pandemic, the Farm Credit Administration (FCA) OIG reported that FCA will require more sophisticated risk evaluation techniques to align with emerging risk factors and identify and deter consequences with the greatest potential impact, which will require using new technologies and developing new skillsets to adapt to oversight challenges. The control environment must also adapt to address increasing expectations associated with internal controls, and FCA must respond and intervene, when necessary, to protect the Farm Credit System.

Working With External Stakeholders

Efforts to coordinate aid and development with external stakeholders and quickly respond to changing priorities, particularly when decisions extend beyond an agency's immediate control and authority, are also constant challenges. The NRC OIG reported that the NRC must engage external stakeholders to ensure transparency of resulting changes to its licensing and oversight processes. In addition, the NRC faces challenges with sustained high-level coordination between the agency and 39 Agreement States to ensure a consistent understanding and implementation of regulations associated with the oversight and waste of certain radioactive materials and limited quantities of special nuclear material.

The USDA OIG reported that it must make significant progress to address past civil rights issues. The USDA OIG found that although the state of Florida invested more than $3.3 million in outreach efforts from 2014 through 2017, sponsors did not consistently ensure that all sites complied with the FNS requirements and guidance related to outreach, promoted the program effectively, or served meals as announced in the state's media campaign. This outcome resulted in the programs' intended recipients—children from low-income areas—potentially not receiving meals. In addition, the USDA OIG reported that the Rural Utility Service and Rural Development can better track their efforts to administer rural infrastructure programs that provide assistance to eligible Native American governments and communities.

The EPA OIG reported multiple issues with state implementation and oversight of drinking water programs. In a 2019 report, the EPA OIG found that the EPA lacked complete and nationally consistent information from states about public water systems' compliance with public notice requirements and cannot fully monitor

compliance and oversee the implementation of this program. In 2018, the EPA OIG concluded that EPA Region 5 did not implement proper management controls that could have facilitated more informed and proactive decisions regarding the city of Flint and Michigan state's implementation of the Safe Drinking Water Act requirements, such as the Lead and Copper Rule.

The USAID OIG reported that USAID actions have the potential to improve interagency coordination, but frequently shifting demands, combined with increasingly uncertain budgets and staffing, will require maximum flexibility to adapt to and advance U.S. foreign policy and national security objectives. Further, the USAID OIG reported that strong planning and monitoring are essential to advance host country self-reliance and safeguard the U.S. Government's foreign development investments. Building appropriate risk mitigation strategies and accountability measures into USAID programs at the start is also necessary to curtail corruption and exploitation and better ensure that programs save lives and improve citizens' well-being. Nevertheless, ongoing imbalances between local capacity and desired outcomes—along with gaps in program planning, monitoring, and assessment—continue to compromise countries' abilities to lead and finance development activities and services after U.S. involvement ends. A lack of sound plans and monitoring has similarly undermined outcomes of USAID's efforts to strengthen health systems, locally led supply chains for global health, education programs in Pakistan, and other development projects. While USAID policy calls for rigorous planning, monitoring, and risk assessments to achieve its foreign assistance goals, USAID OIG audits and investigations continue to identify shortfalls—particularly in policy implementation—that hinder efforts to ensure that U.S. development activities can be sustained after assistance ends.

Collecting and Using Performance-Based Metrics

OIGs reported that, while agencies collect some performance-based metrics, not all collect enough or use the information optimally to ensure mission success. For example, TIGTA reported that the IRS has not yet developed metrics to quantitatively measure its success in detecting and preventing identity theft tax refund fraud. The Legal Services Corporation (LSC) OIG reported that LSC recognizes the challenge that it must collect and effectively use reliable performance and accountability data to assess and demonstrate LSC's and its grant recipients' performance and value to ensure accountability and funder support. The DOT OIG noted that DOT will need to apply sustained management attention to realize performance-based approaches. Likewise, the OPM OIG noted that OPM's budget constraints significantly affect its ability to complete deeper analytics of the drivers of healthcare costs and improved prevention of fraud and abuse.

ABBREVIATIONS AND ACRONYMS

5G	Fifth Generation
AI	Artificial Intelligence
AOC	Architect of the Capitol
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CFO	Chief Financial Officer
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CISA	Cybersecurity and Infrastructure Security Agency
COVID-19	Coronavirus Disease 2019
CPSC	Consumer Product Safety Commission
DHS	Department of Homeland Security
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOI	Department of Interior
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DVE	Domestic Violent Extremist
ED	Department of Education
EPA	Environmental Protection Agency
ERM	Enterprise Risk Management
EXIM	Export-Import Bank of the United States
FAA	Federal Aviation Administration
FAR	Federal Acquisition Regulation
FCA	Farm Credit Administration
FDIC	Federal Deposit Insurance Corporation
FEC	Federal Election Commission
FNS	Food and Nutrition Service
FY	Fiscal Year
GAO	Government Accountability Office
GES	Global Engagement Center
GPO	Government Publishing Office
GSA	General Services Administration
HHS	Department of Health and Human Services
HUD	Department of Housing and Urban Development
HVE	Homegrown Violent Extremist
IG	Inspector General
IG Act	Inspector General Act of 1978
IRS	Internal Revenue Service
IT	Information Technology
ITC	International Trade Commission
LSC	Legal Services Corporation

NARA	National Archives and Records Administration
NASA	National Aeronautics and Space Administration
NLRB	National Labor Relations Board
NRC	Nuclear Regulatory Commission
NSF	National Science Foundation
OIG	Office of Inspector General
OPM	Office of Personnel Management
PBGC	Pension Benefit Guaranty Corporation
PPE	Personal Protective Equipment
PRAC	Pandemic Response Accountability Committee
RRB	Railroad Retirement Board
SBA	Small Business Administration
SSA	Social Security Administration
TFI	Office of Terrorism and Financial Intelligence
TIGTA	Treasury Inspector General for Tax Administration
USAID	United States Agency for International Development
USDA	United States Department of Agriculture
VA	Department of Veterans Affairs