COUNCIL OF THE INSPECTORS GENERAL ON INTEGRITY AND EFFICIENCY

Top Management and Performance Challenges Facing Multiple Federal Agencies

SEPTEMBER 2023

Table of Contents

Introduction

APPROACH TO THIS REPORT

Each year, Federal Inspectors General (IG) 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 third time the Council of the Inspectors General on Integrity and Efficiency (CIGIE) has created a summary of the top challenges facing Federal agencies as identified by those agencies' respective Offices of Inspector General (OIGs).

This report, compiled by a group of 23 individuals from various Federal OIGs, summarizes top challenges that Federal OIGs identified as part of their recent top challenges reports. The resulting top challenges are as follows:

- Information Technology Security and Management (74 percent of respondents).
- Human Capital Management (51 percent).
- Performance Management and Accountability (40 percent).
- Financial Management (39 percent).
- Procurement Management (37 percent).
- Grants Management (37 percent).
- Homeland Security, Pandemic Recovery, Disaster Preparedness, and Climate Change (17 percent).

Information Technology Security and Management

Information technology (IT) security and management 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 are a top challenge because of 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 cybersecurity, modernization of Federal IT systems, IT investment and project management, compliance with regulatory requirements, and increased remote work and web presence after the pandemic.

Cybersecurity

Federal Government agencies are responsible for a vast number of technological resources, including critical infrastructure and sensitive data. For example, the Federal Deposit Insurance Corporation (FDIC) stated it is the custodian of approximately 1.8 petabytes of personal identifiable information. The National Aeronautics and Space Administration (NASA)'s digital footprint includes more than 2,000 public-facing web domains.

Federal agencies are rightly concerned with evolving cyber threats, such as the growth in availability and effectiveness of internet-based hacking tools, threats from foreign adversaries, and quantum-vulnerable cryptographic technologies. For example, the Internal Revenue Service (IRS) sustains more than 1.5 billion cyberattacks each year. The Department of the Treasury (Treasury) stated its staff must be ready to reinforce certain cybersecurity efforts when unforeseen events occur, such as Coronavirus Disease 2019 (COVID-19) and the conflict in Ukraine, or when serious flaws, such as Log4J,[2] are discovered in software or systems. The Department of Homeland Security (DHS) cited the SolarWinds Orion breach, Microsoft Exchange attacks, and the Colonial Pipeline ransomware victimization in its examples of recent threats designed by adversaries to gain unauthorized access to sensitive data, slow or halt Government operations, access intellectual property and research, or gather useful intelligence.

When identifying weaknesses in agency IT environments, many OIGs highlighted identity and access management, administrative privilege control, risk management, and a shortage of technological and personnel resources. With a limited human capital capacity and funding restraints, agencies such as Amtrak and the Denali Commission have had to reduce the scope of some projects or defer delivery dates, which creates a growing backlog for IT security updates. High turnover in key IT positions also leads to insufficient expertise for managing critical cybersecurity functions. For example, the Consumer Product Safety Commission (CPSC) has experienced a turnover in three of the four most key IT security positions in the agency, including the Chief Information Officer. The Federal Election Commission stated it is addressing skill gaps by partnering with DHS and the Cybersecurity and Infrastructure Security Agency to identify and respond to network vulnerabilities while it builds in-house expertise to protect its network. It is also working to seek and adequately compensate industry experts to better compete with the private sector for cyber talent.

FDIC OIG also recommended establishing processes to acquire, analyze, and disseminate cyber threat information from Government partners, databases, and repositories to inform senior officials and decision makers.

In addition to direct cyber threats, agencies also expressed concern with limited vetting and oversight of third-party system contracts and related system development activities. Agencies generally expressed that third-party risk increased during the COVID-19 pandemic as they had to bring external software on board quickly to address the rapidly changing technological environment.

The Small Business Administration (SBA) stated that most of its pandemic assistance was delivered using systems developed by third-party service providers. However, the SBA Business Technology Investment Council did not meet regularly and performed limited reviews of system contracts and related system development activities. In fact, SBA used new outward-facing systems to process large volumes of sensitive data without first conducting baseline control assessments on these systems. SBA's control processes did not identify nor communicate privacy and security risks to decision makers.

As pointed out by the National Credit Union Administration, in some cases, the lack of a direct contractual relationship makes it nearly impossible to accurately assess the actual risk present or determine whether the risk mitigation strategies employed by the third party are adequate and can effectively protect Government data and processes. The FDIC OIG suggested that third-party contracts should include whistleblower provisions to protect contractor personnel who report allegations of contract violations and mismanagement.

IT Modernization

Legacy information systems create the risk of increased maintenance costs, lack of available support, and a decreased capacity to support business needs. Major hindrances to IT modernization efforts across the Government include IT funding shortages, changing priorities, and poor IT investment and project management.

The Treasury Inspector General for Tax Administration has reported that outdated IT systems used by the IRS have caused continued use of paper-based processes, which result in significant delays and contribute to backlogs and poor customer service. The Department of Veterans Affairs (VA) has expressed that its antiquated systems are burdensome, costly to maintain, cumbersome to operate, and difficult to adapt to continuously advancing operational and security requirements.

Current IT modernization efforts are especially focused on cloud-based systems, centralization, automation, and proactive solutions. The Pension Benefit Guaranty Corporation, the Social Security Administration (SSA), and GAO have all expressed an intent to integrate systems and eliminate silos in the technology used to support core agency functions by building end to-end processing systems.

The Office of Personnel Management (OPM) stated it is addressing complaints of ongoing IT funding shortages by allowing unobligated year-end money to be converted to funds for IT modernization. OPM’s Chief Information Officer is taking steps to convert siloed software licenses to enterprise contracts and moving systems to the cloud to reduce IT costs.

Investment and Project Management

Poor IT investment and project management cause inefficient spending, project delays, and sometimes even project failure, which hinders the agency’s ability to meet mission needs, address security risks, meet compliance requirements, and reduce operating costs. Multiple agencies expressed the need for improved transparency and accountability in IT spending to empower agency executives to drive mission value and improve customer experience through technology.

The Railroad Retirement Board stated that no detailed project plans existed for funds marked for IT modernization initiatives, resulting in 94.7 percent of funds being questioned costs. SBA stated that auditors found limited evidence of project performance oversight on IT investments in the last 2 years. The Treasury Inspector General for Tax Administration reported that a project to convert lines of legacy code to a modern software language was initially scheduled to be completed in August 2021 but was pushed back once to September 2022 and then pushed back again, with a planned completion date of April 2023. The report itself was published in early April 2023, so did not confirm if the April date was met.

The Department of Housing and Urban Development (HUD) stated that it has historically failed to fully execute modernization plans and project implementation, failing to realize hundreds of millions of dollars in potential savings and causing ongoing security risks. HUD cited poor contract management and communication; significant weaknesses in cost and schedule estimation processes; and a lack of fully defined roles, responsibilities, and performance measures as reasons for its failures. It also stated that IT project managers often have insufficient expertise or resources for managing the technical aspects, schedules, coordination, and funding for HUD’s IT investments.

GAO stated it is utilizing several methods to improve its IT investment management, including developing leaner products, standardizing project and expectation management, emphasizing scope adherence and customer priorities, and targeting incremental deliverables.

Regulatory Requirements

New regulatory requirements designed to promote security among Government IT systems require agencies to dedicate resources toward adopting new requirements, while maintaining flexibility to adapt to an ever changing IT environment.

Agencies are currently occupied with the requirements of the Office of Management and Budget (OMB) Memorandum M-22-09, “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles.” This memorandum requires agencies to achieve specific zero trust security goals by the end of fiscal year (FY) 2024 and details the specific cybersecurity standards and objectives needed to achieve a Federal zero trust architecture (ZTA) strategy. ZTA is an information system security strategy that continually verifies each user, device, application, and transaction. No actor, system, network, or service operating outside or inside the security perimeter is trusted. The General Services Administration (GSA) and the Department of Health and Human Services (HHS) both expressed that the transition from a perimeter-based security structure to ZTA will require a fundamental redesign of the agencies’ IT security implementations. GSA in particular noted this will require sufficient monitoring of the project to ensure a smooth and secure transition.

In addition to ZTA, agencies cited other regulatory requirements, such as the Federal Information Security Modernization Act, guidance from the National Institute of Standards and Technology and OMB, and diversity, equity, inclusion, and accessibility (DEIA) initiatives. The Treasury expressed concern that dedicating resources to comply with these directives could hamper other IT projects, such as cloud adoption.

Post-Pandemic Remote Work and Web Presence

The COVID-19 pandemic led to a rapid expansion of remote work, increased use of personal devices, and increased demand for customer-facing web portals, especially to compete with private-sector offerings. These challenges heighten many of those already mentioned in this section, with an increased attack surface leading to more cybersecurity risk, a wider range of devices and new technologies causing IT investment and project management challenges, and rapidly issued guidance requiring quick adoption of new requirements.

While the pandemic is no longer at its height, many adaptations made by agencies are ongoing, with increased telework and web presence being top challenges going into 2023.

NOTES

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

[2] Developers use Log4J to keep track of what happens in their software applications or online services.

Human Capital Management

Human capital management includes top challenges related to workforce planning 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.[1]

KEY AREAS OF CONCERN

Key areas of concern related to human capital management include recruiting and retaining a diverse and highly skilled staff, succession planning and knowledge management in a competitive labor market, training and growth opportunities, and strengthening DEIA efforts in the workforce.

Recruiting and Retaining Highly Skilled Staff

Federal agencies have faced challenges attracting and retaining specialized, highly skilled staff in the areas of IT and science, technology, engineering, and math (STEM). The inability to attract and retain the right talent has resulted in skill gaps that affect Federal agencies' ability to meet their various missions. The National Science Foundation reported that it has taken steps to increase participation in STEM among populations that have been under-resourced and underserved. With the move toward increased remote positions, some agencies find it challenging to recruit due to the nature of the work and availability of potential candidates. For example, the Tennessee Valley Authority has remote eligible jobs, but part of the Tennessee Valley Authority's mission pertains to economic development and job creation specifically in the Tennessee valley region.

Another challenge facing agencies is the Federal Government's hiring process—the timeliness of which has been recognized as a detriment to workforce growth and filling key vacancies. The inability to hire required staff directly impacts agency operations, often leading to heavy workloads and burnout, further exacerbating attrition and the need to fill vacancies. In addition, high turnover compromises an agency's ability to retain qualified personnel.

Succession Planning and Knowledge Management

Many agencies have indicated that key drivers of attrition are retirement and limited opportunities for advancement and professional development. Attrition has resulted in a loss of institutional knowledge, subject matter expertise, and gaps in leadership. Retirement or departure of key management and senior employees highlights the importance of succession planning. The

Department of Justice (DOJ) recognized identifying and engaging in successful recruitment and retention policies and practices as a challenge to ensuring the DOJ remains competitive in the labor market. The Partnership for Public Service reported that, as of September 2022, nearly three-quarters of DOJ's Senior Executive Service (73 percent) would be eligible to retire in FY 2025.[2] This may result in a significant loss of institutional knowledge in the coming years.

Furthermore, DOJ does not appear to be prepared to address the potential retirement wave. DOJ OIG reported that DOJ lacked formalized agencywide guidance for "implementing and managing vital approaches to effective and progressive human capital administration." DOJ OIG also found that deficiencies with human resources policies may have caused DOJ components to underutilize compensation and hiring flexibilities available through Direct Hiring Authority, Pathways Programs, and Veteran Hiring programs."[3] To continue to employ a workforce capable of meeting mission-critical agency needs, it is incumbent upon DOJ leaders to engage in succession planning to identify individuals who can assume key roles and responsibilities.

Small agencies face a greater impact when an employee departs the agency. The loss of one employee can be critical, highlighting the need to plan to avoid disruption in agency operations and increasing the need for strong policies, complete records, and standard operating procedures. Succession planning ensures that institutional knowledge and experiences are passed on to new employees.

Knowledge management becomes critical in Federal agencies with high turnover. The Peace Corps has faced higher turnover and brief staff tenure due to its 5-year rule term limit. The lack of institutional knowledge can contribute to inadequate documentation and siloed work practices. Providing staff with training and growth opportunities improves employees' abilities to meet agencies' missions and contributes to retaining skilled employees. Training, growth opportunities, and knowledge management contribute to succession planning. Succession planning allows agencies to preserve institutional knowledge and transfer experience to the new employees, which enables agencies to rely on their subject matter experts. Succession planning better prepares agencies when attrition and retirement occur.

Competitive Labor Market

Federal agencies presently face competition from the private sector as increased wages and workforce engagement make private sector positions more attractive to new and established professionals. A common challenge emphasized throughout reporting agencies is the critical need to ensure the maintenance of a high-quality workforce capable of meeting mission-critical agency needs and, in turn, the needs of the American public. At the root of this challenge is a competitive labor market wherein multiple organizations are contending for the same limited pool of highly skilled candidates. Federal agencies have devised coordinated efforts to effectively right-size the workforce through strategic recruitment efforts focused on targeted recruitment and leveraging hiring flexibilities to attract, onboard, and retain skilled employees.

Recent labor market conditions have provided job applicants leverage to demand competitive pay, benefits, working conditions, and other flexibilities. This is especially true as competition for employees in specialized disciplines, such as STEM, has intensified, often due to Federal Government pay and incentives that are neither competitive nor commensurate with the private sector. The Department of Defense (DOD) indicated it has a gap in the STEM workforce it needs to work on emergent technology and conduct research and development. It has also struggled to recruit and retain a highly skilled cyber workforce. In its top management challenges report, DOD cites a 2021 National Security Commission report, which indicates that the U.S. Government cannot recruit its way out of its technology workforce deficit. The 2021 top challenges report also states, “In 2020, there were more than 430,000 open computer science jobs in the United States; however, there are only 71,000 new computer science graduates from American universities each year.”[4] The problem is further compounded as DOD competes with big tech firms and others within the private sector who can offer more workplace flexibilities and higher pay.

The Election Assistance Commission (EAC), a small agency with the responsibilities of a large agency, reported difficulty filling positions mainly due to salary caps. To address challenges, EAC has utilized remote work to both attract and retain staff, and it is working to propose legislative changes to modify hiring restrictions. The International Development Finance Corporation (DFC) also faces a significant financial hurdle as it works to increase its workforce. Despite being a U.S. financial institute, it is incapable of offering the higher pay rates of other Federal financial institutions, such as FDIC and the Federal Reserve. Financial limitations can create a challenge in retaining employees who can leave for more money and career opportunities. DFC OIG said it intends to assess the extent to which DFC’s pay scale affects its recruitment and retention efforts in comparison to other development finance institutions.

The Department of Transportation (DOT) indicated achieving program goals requires sufficient staff and contractors with the knowledge, skills, and abilities to execute core mission functions and programs. Acknowledging workforce and hiring challenges, DOT officials stated they are working to coordinate across the Department and with OPM to establish additional hiring flexibilities. According to OPM, Federal agencies have discretionary authority to provide financial incentives, such as Federal Student Loan Repayment or retention bonuses, in certain circumstances to support their recruitment, relocation, and retention efforts.[5] Agencies may also offer nonfinancial incentives, such as alternative or flexible work schedules like telework. In spring 2022, DOT implemented new policies expanding hybrid workplace arrangements as part of its post COVID-19 reentry into the office.

A culture of misconduct and distrust may also impact the ability to recruit and retain staff. DOJ highlighted sexual harassment and sexual misconduct as a human capital challenge. Despite multiple efforts, sexual harassment remains a persistent issue. Within the last 5 years, DOJ reaffirmed its zero-tolerance policy and established guidance for responding to substantiated allegations of sexual harassment. The agency has also created a committee to review policies, practices, training, and education. DOJ indicated the agency is committed to fostering a work environment free from misconduct that also ensures equity in hiring and advancement of employees and identifies and engages in successful recruitment and retention policies and practices.

Diversity, Equity, Inclusion, and Accessibility (DEIA)

The cultivation of a diverse workforce is a crucial element for successful recruitment and retention of talented employees, especially in highly competitive markets. To assist in promoting a diverse workforce, the U.S. President has issued multiple executive orders to promote DEIA within the Federal workplace.

DEIA has become a top priority for organizations worldwide, including Government agencies. As such, the top management challenges for the Government in this area are complex and multifaceted. One of the main challenges that Government agencies face is hiring a diverse workforce and creating an environment where all employees feel valued and included. To achieve this environment, agencies must implement policies that promote DEIA, provide training for employees, and hold managers accountable for creating and maintaining an inclusive workplace culture.

Another top management challenge for the Government in DEIA is addressing systemic barriers to inclusion and accessibility. This includes reviewing policies, practices, and procedures that may exclude certain groups of people or prevent them from fully participating in Government programs and services. They may also need to address biases in hiring practices that prevent certain groups from being hired or promoted.

Finally, employees remain the Government's most valuable asset. Agencies must continue to seek ways to remain competitive through compensation and benefits packages and by offering a flexible work environment that promotes work-life balance and helps reduce stress, boosts job satisfaction, and helps employees maintain healthier habits.

NOTES

[1] GAO, High Risk Series, *Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO 21 119SP (March 2021), p. 55.

[2] Partnership for Public Service. *Agency Performance Dashboard – Department of Justice*. Accessed March 14, 2023, from https://ourpublicservice.org/performance-measures/agency-performance-dashboard/profile/DOJ/.

[3] DOJ OIG: *Top Management and Performance Challenges Facing the Department of Justice 2022*, p.42.

[4] *FY 2022 Top Department of Defense Management Challenges* (15 October 2021), p. 83.

[5] https://www.opm.gov/policy-data-oversight/pay-leave/pay-and-leave-flexibilities-for-recruitment-and-retention/ (Accessed Mar. 9, 2023).

Performance Management and Accountability

Performance management and accountability challenges include inter-related top challenges to managing agency programs and operations efficiently and effectively to accomplish mission-related goals. This section emphasizes operational leadership and management challenges, systems of internal control as they relate to overall agency management, enterprise risk, relationships with external stakeholders, and potentially cross-cutting data challenges. OIGs also noted governance challenges in the course of assessing operational concerns and enterprise risk.

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 (ERM), working with external stakeholders, and managing data challenges.

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 Veterans Health Administration plays a critical role in caring for veterans and in supporting our nation's healthcare systems. VA OIG noted incidents and conditions in which quality of care and patient safety have been compromised, leaving veterans harmed or placing them at risk. A contributing factor VA OIG has identified is poor, inconsistent, or ineffective leadership that cultivates a complacent and disengaged medical facility culture in which the Veterans Health Administration goal of "zero patient harm" is improbable, if not impossible. VA OIG noted that a significant concern is governance—the right structures to identify, prioritize, and resolve critical issues.

DOJ OIG's top management challenge report emphasizes the Federal prison system—DOJ's largest employer—noting challenges that include strategic planning, physical safety, longstanding security weaknesses, promoting accountability among staff, and the management of healthcare services. With respect to inmate safety, DOJ OIG also reported a lack of data on deaths in custody and that it sought additional funding to expand the resources it can allocate to the "serious and growing problem" of Federal Bureau of Prisons (BOP) employees allegedly sexually abusing inmates. The Department of Labor (DOL) OIG reported that foreign labor certification programs face the difficulty of balancing a thorough review of visa applications with the need to process these applications timely to meet workforce demands. Moreover, DOL OIG investigations have shown these programs to be susceptible to significant fraud and abuse by perpetrators, including attorneys, labor brokers, employers, and organized criminal enterprises whose activities include human trafficking.

The United States Postal Service (USPS) OIG reported that USPS's processing network operating efficiency could be enhanced. Although USPS has improved service performance for many of its mail products over the past year, performance is still below the goal of 95 percent on-time delivery for most mail products. Amtrak OIG identified employee buy-in to safety management as a key challenge, noting longstanding perceptions that management prioritizes keeping trains running on time over employee safety. Moreover, Amtrak OIG stated that Amtrak has yet to demonstrate that it can consistently manage its key programs and projects to successfully execute them on time and within budget. Amtrak OIG noted that decision makers often do not have the data necessary to make good decisions and that the company has had four chief executive officers since 2016, a challenge to stability.

The Export-Import Bank of the United States (EXIM) OIG reported that poor coordination and dispersed authority continue to be the root cause of some of EXIM's management challenges. Further, agency officials expressed concern that EXIM lacked the corporate processes necessary to ensure transparent, inclusive, and data-driven decision making. The Department of Education (ED) OIG found that ED needs to provide effective oversight of the student financial assistance programs, which requires coordinating and monitoring many Federal, State, nonprofit, and provide entities. HHS OIG reported that HHS is challenged by managing a complex suite of programs with multiple delivery models while also working on strengthening coordination for better programs and services.

Internal Control

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.

OPM OIG reported that fraud, waste, and abuse threaten the financial integrity of OPM's trust fund programs. OPM OIG noted that this is a repeating concern and that aspects of this challenge are consistent across OPM programs. Issues include ongoing threats from program fraud, waste, and abuse; programs that lack adequate controls to support program integrity; and the high costs of improper payments without accurate accounting of improper payment rates. To take one example, the Federal Employees Health Benefits Program (FEHBP) faces ongoing challenges that affect the United States healthcare system generally. Nationwide health trends or crises, such as the opioid epidemic or the recent COVID-19 pandemic, require OPM to act to prevent improper payments while still providing high quality healthcare benefits to Federal employees, retirees, and their eligible dependents. Notably, fraud prevention and program integrity functions in the FEHBP are largely delegated to health insurance carriers. These carriers often further delegate to a complex environment of contractors and subcontractors. This can complicate efforts to prevent fraud, waste, abuse, or patient harm—while improper payments add costs to the FEHBP.

SSA OIG recommended that the agency improve the prevention, detection, and recovery of improper payments. SSA must be a responsible steward of the funds entrusted to its care by minimizing the risk of making improper payments and recovering overpayments when they occur. Even the slightest error in the overall payment process can result in large amounts of improper payments. Per its most recent estimates available, SSA estimated it made approximately

$7.4 billion in improper payments in FY 2021: $6 billion in overpayments and $1.4 billion in underpayments relative to the over $1 trillion in benefit payments it makes annually. SSA OIG noted that SSA has developed strategies to determine underlying causes and determine cost-effective actions to mitigate improper payments.

CPSC OIG reported that the CPSC has not established nor implemented a formal internal control program over its operations. Additionally, there is a misalignment between how the CPSC identifies programmatic or operational activities, how it measures the performance of these activities, and how it reports these activities. Historically, the OIG noted, a recurring challenge at the CPSC, and one which has compounded the difficulty in adequately addressing the CPSC's other internal control deficits, has been the "tone at the top" of the agency. CPSC's senior management officials have repeatedly not held employees accountable for failing to maintain standards.

DFC OIG noted that DFC is created from two predecessor agencies, each with its own mission and culture, presenting a significant management challenge. Strong leadership is needed to continue blending the two predecessor agencies into a new organization with an expanded mission and its own culture. As DFC grows both in staff and portfolio size, DFC must be vigilant to ensure it has strong and effective internal controls and information management systems in place to safeguard its resources and assets, while achieving its mission efficiently and effectively.

NASA OIG highlighted agency challenges in improving the management of major programs and projects because many programs and projects have failed to provide reliable lifecycle costs and schedules. An ongoing challenge for GSA is managing and maintaining effective internal controls. GSA OIG found significant deficiencies in multiple award schedule pricing.

Enterprise Risk Management

An effective 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.

U.S. Agency for International Development (USAID) OIG reported that the agency is challenged to identify and document its risk analysis from the outset of its response efforts in complex emergencies. While USAID has policies that implement requirements to identify and respond to risks throughout a program cycle, recent oversight work on USAID's humanitarian responses highlighted the need for greater attention to managing risk in its programming. USAID OIG specifically noted cash assistance programs in its assessment.

Peace Corps OIG's 2019 management challenges report cites concerns about the agency's struggle to plan for the long-term impacts of risk and resource needs of the organization. Specifically, the Peace Corps OIG highlighted areas of concern for which the agency did not apply sufficient time and resources to ensure access to quality data for decision making and establish oversight to comprehensively consider risks to plan and implement new initiatives and programs. For example, in 2021, the Peace Corps began recording volunteer crime data in a new information system, but historical data was not initially transferred to the new system. The agency subsequently reversed its decision and transferred all the historical data. It also issued new guidance to support the post's site development efforts while crime incident data was transferred to the new system.

SBA OIG reported that risk management needs improvement to ensure the integrity of loan programs. SBA's Office of Credit Risk Management manages lender oversight and credit and compliance risk for the agency's loan portfolio of more than $744 billion, including loans made through the Paycheck Protection Program (PPP). However, those loans are originated by lenders and non-bank lenders with varying degrees of expertise in SBA loan program requirements. Previous SBA OIG audits have found SBA has not adequately recognized or managed significant lender weaknesses. In FY 2020, in an audit of SBA's oversight of high-risk lenders, SBA OIG identified additional internal control weaknesses in lender oversight. SBA has worked to address these issues and strengthen its oversight of lenders. However, SBA still needs to improve, including developing effective oversight policies and procedures and implementing a workflow management tool to interact with its comprehensive portfolio management data warehouse to manage oversight of high-risk lenders.

The Commodity Futures Trading Commission (CFTC) OIG also reported that although CFTC has hired its first Chief Risk Officer, a positive development, the position's reporting relationship is distant from the Commission and the position may be under resourced, thereby presenting challenges to the ERM program's own governance, culture, and operational success. CFTC OIG will continue to monitor the ERM program. Other agencies face enterprise risk in their governance. Farm Credit Administration (FCA) OIG noted that FCA is functioning with fewer than the ideal number of board members. FDIC OIG reported that FDIC Board members and senior officials must implement effective governance to manage risk proactively.

Working with External Stakeholders

Some agencies manage complex stakeholder relationships. Amtrak OIG reported challenges related to relationships with the States, commuter rail agencies, freight rail companies, the Federal Railroad Administration, and Congress. Amtrak has a mixed record managing these key partnerships, including issues with on-time performance and track outages. Amtrak stakeholders face challenges of their own, including pandemic-related budget constraints that influence their relationship with Amtrak. DFC OIG also noted that DFC operates in a complex foreign policy environment and has many stakeholders, both in the United States and around the world, who are interested in what the agency does and how it achieves its goals. DFC faces difficult choices in making investments that balance the competing interests of development impact, foreign policy, and financial performance. Finding the proper balance between these competing priorities presents a significant challenge.

Managing Data Challenges

A number of agencies face distinctive data management challenges, a cross-cutting issue that potentially affects management, internal control, and enterprise risk. OIGs reported that several Federal agencies face data management challenges. For example, ED must have proper controls for data collection and reporting to ensure accurate and complete data. The Equal Employment Opportunity Commission needs to provide resources and management for agencywide training on records management policy and procedures for its digital record management challenge. The International Trade Commission is challenged to manage resources to address its data management issues. The Library of Congress faces challenges in collecting and effectively using reliable performance and accountability data to assess and demonstrate recipients' performances and measure accountability. The National Archives and Records Administration (NARA) faces data management challenges in managing the transition to electronic records and in managing the electronic records archives. DOT OIG reported that the Federal Transit Administration faces the challenge of managing records and sensitive agency information regarding data collection, organization, and standardization.

Financial Management

Financial management involves utilizing management principles for budgeting, forecasting, overseeing, and controlling the Federal Government's financial resources to achieve its obligations to the American people. In addition, the impact of external risks to financial management, such as inflation and social risk, must be addressed.

The financial management challenge identifies concerns related to a wide range of Government functions, from program planning, budgeting, and execution to financial statement reporting, auditing, and oversight. Weaknesses in any of these functional areas limit an agency's ability to ensure that agency revenues and taxpayer funds are used efficiently and effectively. They also constitute a significant risk to Federal programs and operations.

KEY AREAS OF CONCERN

Key areas of concern related to financial management include budget issues, financial reporting problems, and the risk of improper payments. These matters have been exacerbated with the influx of funds from the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), the American Rescue Plan Act (ARPA) and the Infrastructure Investment and Jobs Act.

Adequate Budgets

Budgetary challenges, such as limited appropriations, reduced revenues, increased costs, inaccurate accounting, or wasteful spending, impact many agencies. These challenges affect the ability of agencies to optimally fulfil their mission.

Several agencies reported insufficient funding to adequately carry out their proposed endeavors. For example, CPSC planned for but did not receive a substantial increase in agency funding for FY 2022, affecting its ability to implement plans. The Department of the Interior (DOI) has not had sufficient funding for annual maintenance for its varied resources and assets, which poses a risk to public and employee health and safety. The Federal Labor Relations Authority again did not receive its request for additional funding in the FY 2022 enacted budget. This resulted in a delayed transition to a new agency case management system linked to achieving 100-percent electronic case records.

Other agencies discussed waning revenue, increasing costs, or wasteful spending challenges. USPS continues to be financially threatened by consumer and business behavior changes, increasing competition, growing costs, and mailing and shipping market uncertainty. The Nuclear

Regulatory Commission (NRC) is challenged with developing and implementing the agency's budget in accordance with Federal laws, regulations, and guidance, and maintaining a fee structure that is fair to all types of entities regulated by the agency. Due to increasing healthcare costs, OPM is confronted with keeping health insurance premium rate increases in check while not affecting the level of benefits offered. VA is faced with wasteful spending resulting from supplies, telehealth device plans, or pharmaceuticals that have not been properly managed.

Inaccurate financial information undercuts an agency's ability to plan for and execute its mission activities adequately. The Department of State (DOS) reported that an embassy did not account for costs in accordance with Department regulations. The Railroad Retirement Board was not set up to collect recoveries involving CARES Act benefit payments. Additionally, accounting for earmarks contributed to some of the USAID's mission budgets being out of alignment with the agency's country-specific strategies for self reliance.

Managing the obligation process effectively supports timely execution of mission activities and prevents the loss of funding. At DOS, funds eligible for reclassification were returned to the Treasury primarily because of a lack of procedures to systematically identify and reclassify such funds. For USAID, external considerations can lead to delays obligating funding and restrictions on how funding is spent.

Financial Reporting, Information Systems, and Internal Controls

Financial reporting offers insight and clarity into an agency's financial health and provides information to continuously adjust its operations. A financial information system (FIS) is a type of business software utilized in the organized process of collecting and analyzing financial data for optimal financial planning, forecasting decisions, and helping an agency achieve its financial objectives. Internal controls are designed to protect and improve the accuracy and transparency of financial reporting data. Proper financial management and oversight can be crucial in ensuring an agency's programs achieve the intended benefits.

In these three areas of concern, DOD continues to have ongoing challenges. For example, DOD faces significant challenges related to financial management and budgeting due to its size and complexity. Its current budget processes and systems have shortcomings, such as ineffective processes and controls for reconciling Fund Balance with Treasury. DOD relies on more than 250 information systems and continues to use manual processes rather than automated and sustainable processes. This is despite spending billions over the last decade to implement modern enterprise resource planning systems.

During contracted financial statement audits overseen by DOD OIG, DOD had many findings, such as the agency's inability to provide all the transactions reconciled to its accounting records and accurately value its general property, plant, and equipment assets. In addition, DOD's financial statements did not include the Joint Strike Fighter Program, despite its value exceeding $1 trillion, with each F-35 aircraft costing more than $70 million. DOD is still the only agency that has never been capable of accurately accounting for and reporting on its spending or physical assets.

DOD's failure to produce reliable financial statements is a major factor in the Consolidated Financial Statements of the U.S. Government receiving a disclaimer of opinion each year.[1] DOD also struggles to meet the November 15 deadline, established by OMB, for issuing agencywide financial statements.

DOS also has issues with financial reporting and internal controls. Some DOS bureaus did not consistently use the proper general budget object code designations in accordance with requirements when recording expense transactions. In addition, significant numbers of personal property transactions were not recorded in the correct fiscal year, resulting in misstatements. Until deficiencies are addressed, DOS will not fully understand its spending patterns for billions of funds.

DOS also lacks quality assurance. Because DOS does not certify overseas transactions, auditors could not assess the quality of the data that DOS submitted. Likewise, lapses in recordkeeping and appropriate physical security controls contributed to missing items of significant value from its gift vault.

At DHS, auditors found weaknesses in FIS and financial reporting. DHS continues to make progress meeting Digital Accountability and Transparency Act of 2014 (DATA Act)[2] requirements, but system limitations hinder the Federal Emergency Management Agency's (FEMA's) ability to track spending of roughly $45.5 billion in COVID-19 funding associated with the response to the pandemic.

DHS has taken steps to deploy a modernized financial management system as an effort to mitigate underlying causes of FIS and financial reporting material vulnerabilities. These efforts also aim to make spending information more transparent. DHS still needs to implement and consistently use the Governmentwide financial data standards to improve the accuracy in reporting certain data elements to fully achieve the DATA Act's objective. Furthermore, FEMA needs to strengthen its fraud preventive controls.

Risk of Improper Payments

An improper payment is any payment that does not meet statutory, contractual, administrative, or other legally applicable requirements and may be an overpayment or underpayment. Reducing improper payments, such as payments to ineligible recipients or duplicate payments, is critical to safeguarding Federal funds.

Many agencies had issues with improper payments. For example, FEMA did not implement controls to prevent the State Workforce Agencies from paying more than $3.7 billion in potentially fraudulent and improper payments through its Lost Wages Assistance program. FEMA relied on weak underlying unemployment insurance program controls, such as self-certifications, to determine eligibility and prevent fraud. These weak controls allowed ineligible and potentially ineligible DHS employees or individuals using their identities to receive Lost Wages Assistance. FEMA needs to strengthen its fraud preventive controls when determining claimant eligibility because the reliance on self-certifications continues to lead to billions of dollars in potentially fraudulent and improper payments.

Similar to FEMA, DOL is estimated to have improperly paid $163 billion in unemployment insurance benefits; this improper payment is attributable to fraud. DOL OIG noted that some State Workforce Agencies suspended benefit payment controls and reassigned benefit payment control staff to process unemployment insurance payments and faced impediments with insufficient IT systems.

While the Defense Intelligence Agency (DIA) has complied with the Payment Integrity Information Act (PIIA), DIA OIG found that the agency did not revise its payment integrity standard operating procedures to incorporate the latest changes to PIIA and OMB policies. DIA OIG also noted that the updated procedures may help DIA mitigate risks of future noncompliance with PIIA requirements.

The Federal Aviation Administration (FAA) reported improper payments of $3 million related to the CARES Act. These improper payments arose from increased workloads due to the COVID-19 pandemic. Program officials had to review more transactions in less time, resulting in a decrease in the quality of the reviews.

Another instance of the lack of sufficient internal controls that led to improper payments occurred at EXIM. EXIM OIG found that EXIM's procurement practices made improper awards of approximately $4.1 million in contract task orders.

HHS programs account for some of the largest estimated improper payments in the Federal Government. In FY 2021, Medicare, Medicaid, and the Children's Health Insurance Program together accounted for 55 percent, or $153.7 billion, of all Governmentwide estimated improper payments reported. HHS OIG noted that insufficient oversight of grant programs and contracts poses risks of significant improper payments.

SSA is responsible for issuing over $1 trillion in benefit payments annually. According to SSA OIG, improper payments may occur when SSA makes mistakes in computing payments or fails to obtain or act on available information. For example, in FY 2022, SSA employees incorrectly input student information on beneficiaries' records, which resulted in SSA underpaying an estimated 14,470 beneficiaries approximately $59.5 million. Unfortunately, SSA's automated systems could not compute benefit payments due in certain situations, and SSA did not provide employees with a comprehensive tool to manually calculate these payments.

Because SSA must expend extra resources to process additional payments to remedy underpayments, SSA OIG noted that obtaining data from external sources, such as other Federal agencies, State agencies, and financial institutions, is critical to preventing and detecting improper payments.

The above examples include just a few of the agencies facing adequate budget issues, financial reporting problems, outdated FIS, internal control deficiencies, and the risk of improper payments observed as aspects of Financial Management Challenges.

NOTES

[1] A disclaimer of opinion means that auditors are unable to obtain sufficient evidence on which to base an audit opinion.

[2] The DATA Act directs the Federal Government to standardize and publish a wide variety of reports and data in order to foster greater transparency over federal spending. The law requires the Treasury to establish common standards for financial data provided by all Government agencies and to expand the amount of data that agencies must provide to the Government website, USASpending.gov.

Procurement Management

The procurement management challenge encompasses the entire procurement process, including contract award and post-award contract administration. Given that the Federal Government awarded more than $665 billion in contracts in FY 2020,[1] 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 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 and reviewing invoices and payments.

Contract Award Process

Federal agencies face challenges in maintaining robust oversight of contract portfolios and contract execution and performance. Thorough documentation and performance monitoring are essential to ensure agencies comply with all applicable regulations and receive a fair return from their contract vendors. Deficiencies in these areas of contract administration can lead to violations of contract terms and to potential cost premiums.

Recent DOJ OIG reports have shown these issues are prevalent in the procurement of medical services and IT. For example, the DOJ OIG's March 2022 audit report regarding comprehensive medical services contracts awarded to a university medical school states that BOP officials lacked sufficient data to monitor the contracts and did not maintain adequate documentation for contract modifications in accordance with the Federal Acquisition Regulation (FAR). Similarly, in a February 2022 audit report, the DOJ OIG notes that the contract files of an FBI purchase order with a ceiling of $87.5 million lacked required documents and sufficient detail to support the rationale for pertinent decisions throughout the purchase order lifecycle.

FDIC OIG determined its agency had limited data and reporting capabilities for agencywide oversight of its contract portfolio. FDIC OIG found FDIC was overseeing acquisitions on a contract-by-contract basis rather than on a portfolio basis. Therefore, FDIC did not have an effective contracting management information system to readily gather, analyze, and report portfolio-wide contract information across the agency. Although OIG recommended FDIC provide enhanced contract portfolio reports to FDIC executives, senior management, and its board of directors, this recommendation has remained unimplemented since FDIC OIG issued the report more than 3 years ago.

Oversight is also required to determine whether applicable laws and regulations are followed and whether the contractor complies with contract requirements. DOS OIG identified similar contract oversight deficiencies while auditing security, construction, and facility and household services contracts at overseas posts. DOS OIG found contractors did not always establish and maintain trafficking in persons (TIP) compliance plans in accordance with FAR requirements, and department Contracting Officer's Representatives did not always request and review the TIP compliance plans to develop required TIP monitoring strategies. Furthermore, Department contracting personnel did not consistently implement management controls for monitoring contracts to ensure contractors do not engage in unlawful TIP practices.

Invoice Pricing and Payment Review

OIGs have continued to report instances where agencies fail to appropriately review invoices and track associated payments to ensure the Government received the goods and services, for which it had contracted and paid, at a reasonable price. For example, DOT OIG found that FAA modified policy to lessen supporting documentation requirements for CARES Act funds, which expedited reviews but adversely impacted the agency's ability to assess eligibility and validity. In another review examining a limited number of IT shared service invoices, DOT OIG identified $4.3 million in unsupported and questionable contractor charges.

In recent years, DOD has found it more difficult to determine whether it is paying a fair and reasonable price for the items it buys. Previous National Defense Authorization Acts broadened the definition of a commercial item and required DOD to use commercial buying practices. Corresponding changes to the commercial section of the FAR require DOD to continue to purchase an item commercially if it has previously purchased the item that way. The consequence of these commercial buying practices is that contractors can deny DOD access to cost and pricing data related to that item, which contracting officers need to determine whether the contractor is charging the DOD a fair and reasonable price.

These deficiencies heighten the risk of fraud, waste, and abuse, and may hinder the ability of an agency to complete its mission, as finite resources may be lost to mismanagement.

NOTE

[1] This information comes from a GAO infographic. In FY 2020, the Federal Government spent more than $665 billion on contracts, an increase of over $70 billion from FY 2019. Half of this increase, or $35 billion, is attributed to spending on medical supplies and pharmaceuticals to treat COVID-19 patients, among other things related to COVID-19.

Grants Management

The Federal Government has been issuing grants for centuries. Every such funding opportunity comes with requirements applicants must follow, and Federal agencies are tasked with ensuring that grant recipients abide by those requirements. Challenges Federal agencies face with grants include the proper awarding of funds; the oversight, integrity, and accountability in the use of grant funds; ensuring grants achieve intended results; the risks associated with rapid grant funding growth, including the need for upgraded management information systems; and the management of grants related to the COVID-19 pandemic.

The top 10 Federal agencies issued $1.1 trillion across 525,604 grants in FY 2022 according to USAspending.gov. This amount is a drop from FY 2021, when agencies issued $1.3 trillion across 576,797 grants. The largest grant issuing agency by far is HHS, with more than $740 billion in grants. Other agencies in the top 10 include DHS, DOD, DOL, DOT, ED, USAID, HUD, Department of Agriculture (USDA), and the National Science Foundation.

KEY AREAS OF CONCERN

Key areas of concern related to grants management include ensuring funds are awarded and spent appropriately; Agency oversight, integrity, and accountability on the use of grant funds; ensuring grant investments achieve intended results; and risks associated with the rapid changes in grant funding.

Ensuring Funds are Awarded and Spent Properly

With more than a half million grants issued in FY 2022, agencies can experience challenges ensuring that their personnel follow all rules when awarding grants. A continuing challenge for the Federal Government is ensuring agencies spend taxpayer dollars prudently and safeguard programs from fraud, waste, and abuse. Inappropriate, illicit, and misuse of grant funds not only strips needed projects from State and local communities, but overburdens and redirects agencies' limited resources away from supporting public initiatives.

Since FY 2015, Congress has appropriated funds for the Office of Community Oriented Policing Services (COPS) to award competitive Anti-Heroin Task Force Program grants to State law enforcement agencies with high rates of primary treatment admissions for heroin and other opioids to investigate, through Statewide collaboration, the unlawful distribution of heroin, fentanyl, carfentanyl, and prescription opioids. From 2015 through 2021, COPS awarded $135 million in grants through this program.

DOJ OIG found that COPS did not have a written standard operating procedure to guide how its separate divisions need to work together to administer and oversee these grants. Additionally, HHS OIG determined that due in part to the agency's size and in part to some programs having error rates that exceed statutory benchmarks, HHS programs account for some of the largest estimated improper payments in the Federal Government. Medicare, Medicaid, and the Children's Health Insurance Program together accounted for 55 percent, or $153.7 billion, of all Governmentwide estimated improper payments reported in FY 2021. Furthermore, insufficient HHS oversight of grant programs and contracts poses risks of significant improper payments. Additionally, HUD OIG found the agency faces the challenge of effectively collaborating with other agencies and service providers to ensure that grantees and subrecipients understand all available funding options, as well as the restrictions and rules that govern each funding source. Inefficient cross-collaboration increases the risks of improper award funding due to coordination issues and overlapping services.

Oversight, Integrity, and Accountability on the Use of Grant Funds

Given the large number and dollar amount of grants, agencies continually face challenges tracking the proper uses of grant funds. The Federal Government expectation is that Federal agencies will oversee and monitor their entire grant program cycle, including grantees and subgrantees. Federal agencies' reliance on grantees to monitor subgrantees and subrecipients places agencies in a diminished capacity to identify weaknesses, in the multilayered processes and procedures inherent in grant funding, to reduce the risks of fraud.

ED OIG stated that the Department should focus on the actions taken bypass-through entities to provide oversight of their subrecipients and take steps to ensure that its technical assistance and monitoring activities are both risk based and data driven. The Department of Commerce OIG noted that administering grant programs requires implementation of internal controls to ensure that it meets program goals and uses funds appropriately.

For grant programs, this includes providing oversight and guidance to award recipients, as well as ensuring that grantees and subgrantees have the appropriate certifications for requirements that are material to grant award decisions. DOI OIG noted that with disaster relief funding, those emergency funds received by the agency are of significant risk because of the speed of the award "without competition," which requires increased oversight to control misuse and fraud. DOI lacked effective oversight and failed to comply with Federal regulations for grants awarded using emergency funds.

Finally, USDA OIG found that the agency's internal controls on specific programs for over 8 years continued to lack efficiency and effectiveness, which diminished the agency's ability to detect fraud and waste. USDA OIG did identify a success with the agency's "process improvement for enhanced integrity" in the USDA's Rural Development's Community Facilities Direct Loan and Grant Program. The agency was able to safeguard the integrity of a substance use disorder facilities requirement in compliance with the Agriculture Improvement Act of 2018 due to its process improvements.

DOT noted the agency monitors a higher level of grant funds, which presents challenges to the agency's financial management. Improving grant monitoring procedures, consistent oversight, and maintaining controls to detect, prevent, and reduce inappropriate payments is critical to help the agency safeguard assets. Therefore, DOT's FY 2023 plan includes ongoing and intentional efforts to conduct fraud risk assessments of Grants Management Process Reviews evaluating the design of program pre award and post-award internal controls.

Ensuring Grant Investments Achieve Intended Results

Congress looks to agencies to ensure grants and grantees are achieving intended results. To achieve this outcome, agencies must ensure performance measures are part of all grant agreements. Unfortunately, OIGs have found their agencies' grant management systems were not adequate to account for and were vulnerable to a significant emergency such as the COVID-19 pandemic and unprepared for the subsequent CARES Act funding response that followed.

HUD OIG noted several instances of grantees misusing funds for unauthorized and ineligible activities because of the HUD's struggle with creating and sustaining grant management systems. For example, a grantee paid $1 million dollars to resolve allegations that they used HUD funds for unauthorized purposes. Due to that fraud, the local citizens never received funds to improve the community as intended. SBA OIG reported that program officials established performance goals and indicators for the supplemental CARES Act funds provided to Small Business Development Centers, Women's Business Centers, and the Resource Partner Training Portal, but SBA should have clearly defined the goals and set targets to ensure they were achieved effectively as intended.

Finally, USDA OIG emphasized the USDA's need to increase its monitoring and reviews to capture metrics on programs performance to effectively evaluate their progress. USDA OIG identified some programs had no performance measures in place, leading to unreliable data used by USDA to assess benefits to recipients. DOL OIG noted that in March 2022, it issued an advisory report to the agency of an aggregation of reports from the past decade that identified the following weakness in the agency's grant program: awarding grants, reviewing grantees' use of funds, and measuring grantee performance.

Risks Associated with the Rapid Changes in Grant Funding

Agencies can receive dramatically different amounts in grant funding year to year. Especially when grant funding increases rapidly, agencies can struggle to distribute the grant funding within allotted timeframes. Furthermore, agencies continuously fight to dedicate qualified and effective oversight resources to address grant fund management.

The Denali Commission OIG noted that the agency experienced a significant decrease in funding in recent fiscal years, from receiving about $141 million in FY 2006 to about $25 million in FY 2019, a decrease of approximately 82 percent. However, the recently passed infrastructure bill provided a one-time appropriation of $75 million that reversed the last reduction. Since March 2020, the CARES Act and ARPA have made available to HUD $14 billion in supplemental Community Development Block Grant (CDBG) funding for grants to current formula grantees to prevent, prepare for, and respond to the COVID-19 pandemic, such as CDBG CARES Act, Emergency Solutions Grant CARES Act, and HOMEARP awards.

HUD OIG found that HUD struggled to provide reasonable oversight, monitoring, and staffing for these enormous financial awards, especially the Office of Block Grant Assistance. The Office of Block Grant Assistance oversees more than 1,200 grant programs along with the pandemic programs mentioned above. Lastly, in FY 2021, pandemic relief legislation authorized new, multibillion-dollar grant programs in addition to SBA’s existing entrepreneurial development grant program portfolio. Congress had authorized $45.3 billion for SBA to administer as grants to provide economic relief and technical assistance, nearly doubling SBA’s existing technical assistance programs. DOT OIG noted that the agency needed to hire over 1,000 employees, which includes grant managers to oversee the grant programs, outreach, and monitoring of documentation supporting grant expenditures.

Homeland Security, Pandemic Recovery, Disaster Preparedness, and Climate Change

The homeland security, pandemic recovery, disaster preparedness, and climate change challenge includes new and expanded top challenges related to preventing and disrupting terrorist attacks, the pandemic's effect on evolving agency operations, planning for and protecting against manmade and natural hazards and disasters, and the growing impact of climate change. This challenge reflects the evolving environment affecting the United States and Federal agencies charged with executing missions related to homeland security, pandemic recovery missions, and disaster preparedness, including the impact of climate change. Since 2020, the worldwide outbreak of COVID 19 has placed significant strain on Federal agencies' 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, pandemic recovery, disaster preparedness, and climate change include countering terrorism and defending the homeland against security threats, responding to and adapting work practices caused by the pandemic and related funding issues, including fraud, preparing and responding to disasters, and the impact of climate change.

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. According to DHS OIG, 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.

In addition, EAC provides guidance and best practices to States and U.S. territories to assist in their administration of Federal elections, acting as a customer service agency rather than a regulatory agency. The Help America Vote Act mandates that EAC serve as a national clearinghouse and resource for the compilation of information with respect to the administration of Federal elections, but Section 209 is clear about the limitations on rulemaking. As part of this role, EAC is a conduit for information to flow to State and local election officials, including information about the election system's place in the Nation's critical infrastructure—a determination made in 2017.

Among agencies' highest priorities are countering threats posed by foreign and domestic terrorism. DOJ OIG stated that, domestically, the United States faces threats by both homegrown violent extremists and domestic violent extremists. According to a DOJ OIG report, many of the challenges associated with the use of cryptocurrency transcend the cyber-realm, as criminals increasingly use cryptocurrency to purchase deadly weapons, support terrorism, sell and purchase narcotics and child pornography, and engage in human trafficking activity, all of which have severe ramifications of their own. Tracing and understanding cryptocurrency transactions, as well as seizing cryptocurrency used in illegal activity, are components of DOJ's efforts to combat cybercrime and crimes facilitated by it.

According to DOD OIG, combating terrorism, whether on the battlefield or through anti-money laundering and combating terrorist financing operations, remains critical to addressing this challenge. 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. DOD has incrementally reduced its personnel and resources deployed for counterterrorism missions around the world during the last several years and has shifted to address the re-emergence of nation-state actors. Therefore, 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.

Currently, banks are facing a rising interest rate environment while the U.S. economy faces inflationary pressure, and continued uncertainties remain resulting from Russia's invasion of Ukraine. Banks have also adopted new technologies and third-party partnerships to engage customers during increasing cybersecurity breaches. Banks are also entering into markets for digital assets, which may increase money laundering and terrorist financing risks.

During the past year, the Office of Terrorism and Financial Intelligence has remained dedicated to countering the ability of financial networks that support terrorists, organized transnational crime, weapons of mass destruction proliferators, and other threats to international security through intelligence analysis, sanctions, and international private sector cooperation. As previously reported, identifying, disrupting, and dismantling these networks continue to be challenging as the Office of Terrorism and Financial Intelligence's economic authorities are key tools to carry out U.S. policy. Additionally, criminals and other bad actors evolve and continue to develop more sophisticated money laundering methods in an attempt to avoid detection. To help stem the flow of opioids shipped to the United States through the mail, Congress passed the Synthetics Trafficking and Overdose Prevention Act of 2018.

The law requires all postal packages entering the United States from international posts to have Advance Electronic Data. Advance Electronic Data refers to electronic messages with information about cross-border packages and the larger shipment with which the package was sent. USPS receives these data from sending posts and forwards it to Customs and Border Protection before packages reach the United States. Customs and Border Protection uses Advance Electronic Data to identify packages that might contain illicit items, such as drugs and counterfeit merchandise. The United States Postal Inspection Service also serves a role in addressing narcotics and other criminal activity. Criminal investigations and data analytics are continuing to address the problem of narcotics in the mail.

Cyber and physical security threats present a persistent challenge to the safe and reliable operation of the nation's electric power generation and distribution system. As the primary regulator of the Nation's commercial nuclear power fleet, NRC must maintain robust and adaptive oversight programs to ensure nuclear power licensees can protect their facilities effectively against evolving threats and a broad spectrum of potential adversaries, including competitor nation states, organized criminal groups, and domestic terrorists. In September 2021, NRC issued a baseline inspection procedure for biennial oversight of nuclear power licensee cybersecurity programs that started in January 2022. NRC began implementing the new nuclear power cybersecurity inspection procedure biennially and incorporated these inspections into the Reactor Oversight Process.

In addition, GSA must manage the risk that prohibited items could be offered under any of its thousands of Multiple Award Schedule contracts. The possibility that customer agencies could purchase and use the prohibited items poses a national security risk to the Government. Further, GSA plays a significant role in providing a safe, healthy, and secure environment for Federal employees and visitors at over 8,300 federally owned and leased facilities nationwide. Additionally, in accordance with a September 2018 memorandum of agreement with DHS, GSA is responsible for the installation, maintenance, and repair of approved security fixtures, including physical access control systems.

Responding to and Adapting Work Practices Caused by the Global Pandemic

Responding to the COVID-19 pandemic has presented significant challenges for Federal agencies, most notably in ensuring the continuity of operations and services while overcoming technological challenges, challenges related to fulfilling agency missions while expanding remote work, and staff retention and recruitment challenges. As a result of pandemic shutdowns, many agencies took 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. Shifts to more in-person work, combined with competitive job marked pressures, have negatively impacted employee morale and staffing at many agencies.

Finally, agencies developed large-scale work from-home operations to continue operations during pandemic-related shutdowns, and the increase in remote access to IT systems also increased the risk of security breaches. As mass telework continues at many agencies, they have overcome some of these challenges, but their pandemic response has highlighted how some agencies' IT services were fragmented or needed modernization to perform optimally. IT challenges are discussed in further detail in the Information Technology and Security Management section of this report.

Many agencies also face challenges in ensuring stability and full and effective functioning of its components because of COVID-19 and related work adaptations. For example, the pandemic delayed FAA air-traffic controller training critical to certify personnel and maintain knowledge and skills. Significant staffing shortages have also hampered the IRS's ability to process tax returns, issue refunds, and provide taxpayers with timely assistance. Many agencies reported that remote and hybrid work adaptations have strained abilities to manage contracts and grants, coordinate operations with other agencies and stakeholders, complete infrastructure projects, and to monitor and guide operations when staff could not be physically present to do so.

Effective service provision has had significant impacts on the ability of healthcare agencies to meet their missions. The U.S. Navy has reported that pandemic-related deployments and support for the nationwide vaccination effort resulted in reduced healthcare services for beneficiaries. In April 2022, DOD OIG reported that increased workload related to pandemic response exacerbated existing healthcare staff shortages. Overall, the COVID 19 pandemic increased demands on DOD healthcare personnel, contributing to understaffing and burnout. These factors affect the readiness of DOD healthcare personnel and their ability to deliver care effectively.

DOD OIG plans to assess how healthcare staffing shortages affect overall military readiness and strategies to mitigate these shortages in future pandemics. VA OIG highlighted that staffing shortages and workforce fatigue have inhibited its ability to provide care, while referral backlogs resulting from the pandemic have increased the demand for care in the community. These factors have also strained the VA's ability to coordinate care with community providers. According to DOJ OIG, the pandemic also affected BOP's ability to mitigate health risks at facilities while dealing with staffing shortages. The impacts to BOP operations continue, and all institutions currently operate at modified levels.

As COVID-19 related shutdowns have ended, many agencies have struggled with whether and how to shift back to more in-person office work. While many agencies have developed robust permanent telework policies, some have experienced disagreements among stakeholders regarding expanded or permanent remote work. As a result, agencies have experienced decreased employee morale, resistance to returning to in-person work, and increased attrition among experienced staff. These factors have exacerbated challenges to fulfilling agency responsibilities.

Agencies have implemented many different return-to-work strategies with varying success and impacts on operations. SSA reduced staff telework as pandemic-related shutdowns eased but still attempts to accommodate staff by allowing telework 2 days per week. Despite this, SSA has experienced an increase in employees requesting reasonable accommodations to delay in-person work, which impacts its ability to serve beneficiaries. Meanwhile, DOS reported positive outcomes from the transition to hybrid work environment and increased flexibilities, and the Department aims to maintain these flexibilities going forward.

Competitive job market pressures and challenges with instituting permanent flexible work policies have also contributed to staffing shortages at several agencies. Agencies have experienced heightened competition for employees as many private-sector companies offer fully remote work opportunities. These pressures, combined with related employee attrition, have further impacted agency operations. For example, USPS has experienced consistent understaffing since the onset of pandemic shutdowns—contributing to delays and increased overtime. A broader discussion of human capital challenges is in the Human Capital Management Section of this report.

Staffing shortages and hiring difficulties have affected agencies in various ways. For example, NARA reported significant, adverse impacts on the ability to provide access to military service records to veterans. NARA estimates it will take 6 months to a year to achieve full staffing levels, which would then take a year to resolve its backlog of requests. Following EXIM's return to work, employees reported decreased morale, and some reported that they left the agency due to their unwillingness to work in the agency's physical workspace. At BOP, the pandemic caused significant shifts in staffing responsibilities, and according to DOJ OIG's February 2021 survey, 66 percent of BOP staff respondents said they were required to perform tasks outside their normal duties, 28 percent were required to work longer shifts, and 23 percent took leave to recover from increased work demands. These results and opportunities for remote or hybrid work outside BOP further pressure the BOP's abilities to meet its mission.

Administering Pandemic-Related Funding

The CARES Act was enacted in 2020 and ARPA was enacted in 2021 because 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. ARPA included economic relief and stimulus to address the continuing impact of the pandemic on the economy, State and local governments, individuals, and businesses. Consequently, the additional responsibilities resulting from these two Acts, and their provisions, such as PPP, continue to pose challenges for Federal agencies, as they must effectively administer and monitor grant programs and take additional proactive steps to create and sustain a culture of fraud prevention, while also continuing to execute their normal agency missions, including disaster recovery.

The supplemental funding added many new responsibilities to Federal agencies that required additional resources or procedures. For example, DOT's surface transportation agencies had to implement new formula and discretionary grant programs, increase broader access to DOT funding and programs, enhance project flexibility and environmental reviews, and facilitate changes to specific Federal project requirements. DOT will face challenges in dedicating qualified and sufficient resources to provide sound contract and grant stewardship. SBA disbursed CARES Act funds through the PPP and the Economic Injury Disaster Loan program in amounts unprecedented in SBA's history, but the absence of a proper control environment led to significant fraud risk and vulnerabilities.

According to the IRS, ARPA modified several credits, including expanding the Child Tax Credit. Determining eligibility for and the amount of the Child Tax Credit is a complex process and required a significant undertaking on the IRS's part, as it needed to develop processes and procedures to determine eligibility, compute advance payment amounts, and develop an online portal and nonelectronic assistance options for taxpayers to provide the IRS with updates to key information used to compute the advance payment amounts.

Implementation of the pandemic relief laws poses challenges for ED, as it must effectively oversee and monitor new grant programs and additional Federal education funds as it oversees more than 100 other grant and loan programs. According to the Food and Nutrition Service, the CARES Act increased the Emergency Food Assistance Program funding to more than $1.2 billion, thus increasing the potential risk that food assistance may not go to those in need.

Due to the additional funding and reporting requirements associated with the CARES Act and ARPA, the National Endowment for the Arts will be challenged with timely review of grantees' increasing number of reimbursement requests and the National Endowment for the Arts processing and disbursement of CARES Act and ARPA funds. Grant management challenges are discussed in further detail in the Grant Management section of this report.

Pandemic-Related Fraud

The past years of COVID-19 have shown Federal agencies that bad actors will always try to take advantage of Federal programs. OPM identified the FEHBP as vulnerable, whether through defrauding and harming its beneficiaries or the program itself. The ability to respond to these threats is critical to protect taxpayer dollars and FEHBP members' health. The widespread, entangled, and layered web of fraud, waste, and abuse has created vulnerabilities that could potentially be mitigated by a centralized Program Integrity Office.

The banking sector also faces risks related to the Government's response to the pandemic crisis. FDIC reports that the PPP has been administered through the Nation's banks. It is estimated that fraud in the PPP could be as high as $117.3 billion, and banks may suffer losses resulting from fraudulent loans.

The IRS continues to work diligently to combat various scams designed to steal taxpayers' money or personal information. In 2022, the IRS added pandemic–related scams to its "Dirty Dozen" list of a variety of common scams that taxpayers may encounter. These scams involve the theft of a person's money and identity with bogus emails, social media posts, and unexpected telephone calls, among other things. The scams can take a variety of forms, including using unemployment information and fake job offers to steal money and information from people. All of these efforts can lead to sensitive personal information being stolen, with scammers using it to try to file a fraudulent tax return, as well as harming victims in other ways.

Preparing for and Responding to Disasters

Responding to increasingly frequent disasters that grow in magnitude has presented immediate and significant challenges for Federal agencies, most notably with managing funding increases and incorporating emergency planning.

For instance, HUD is challenged to implement disaster recovery programs that come with large funding increases without a commensurate level of structure and oversight funds and set program standards on a disaster-by-disaster basis using complex allocation notices. Following a disaster, HUD's long-term role is to address unmet needs in communities after initial emergency disaster relief efforts have ended. HUD provides disaster recovery assistance primarily through the CDBG-Disaster Recovery program. HUD's disaster recovery programs continue to evolve as the types of disasters are increasing in magnitude and frequency and as mitigation becomes an additional focus for the programs. In addition, HUD has had to adapt its disaster assistance to encompass novel disaster circumstances and events.

NRC stated that natural disasters, such as hurricanes, floods, and wildfires, present ongoing operational risk to NRC licensees. The agency can prepare for events of similar or greater impact by incorporating lessons learned during its COVID-19 response into routine policies and procedures, as well as the agency's contingency planning.

DOI received $635.9 million in disaster relief funding in FY 2022. These funds are available for emergency response activities related to drought, wildfires, hurricanes, and other natural disasters. Financial awards for emergency response activities are generally high risk because they are awarded quickly and often without competition, requiring enhanced oversight. DOI will continue to face challenges managing its contracts and grants to prevent fraud, waste, and mismanagement, particularly with the significant increase in funding opportunities.

DOS OIG assesses emergency action planning as part of this challenge. Department guidelines require U.S. embassies to maintain post-specific emergency action plans to respond to situations such as bombs, fires, civil disorder, or natural disasters. DOS OIG continues to highlight deficiencies that have significant safety implications or are related to crisis management preparation. Architect of the Capitol OIG continues to note issues with emergency preparedness consistency and implementation across the campus. The events at the U.S. Capitol on January 6, 2021, and other persistent threats against the Capitol campus highlight the need for sustained emergency preparedness and smart processes for accessing its many buildings and structures.

According to DHS, COVID-19 response and recovery is the largest relief assistance program in American history. FEMA, as the lead response agency, has been charged with administering and overseeing $45 billion in CARES Act funding. Further, FEMA has recently been charged with administering $6.8 billion in Infrastructure Investment and Jobs Act funding. In addition, DHS seeks to achieve specific objectives related to strengthening preparedness and resilience. FEMA struggles with ensuring disaster grant recipients and subrecipients understand and comply with relevant authorities governing grants and assistance. FEMA has also proven susceptible to widespread fraud and made billions in improper payments. DHS OIG continues to identify persistent, systemic shortcomings in FEMA's disaster response and recovery efforts. DHS OIG has published a significant body of work recommending improvements in Federal disaster response and recovery efforts.

Impact of Climate Change

Changing climate patterns, extreme weather events, and global pandemics have long-term impacts on Federal agencies' personnel and their ability to execute their missions and the economy. 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 USAID, must also develop plans and procedures to guide the reentry of their domestic and overseas workforce as pandemic conditions allow.

According to the Environmental Protection Agency, the increased incidence of disasters due to climate change creates potential vulnerabilities that must be identified and addressed. For example, facilities regulated by the Environmental Protection Agency, such as chemical manufacturers, hazardous waste handlers, underground storage tanks, and contaminated sites, pose a risk of uncontrolled releases of harmful chemicals and contaminants due to increases in natural disaster incidents caused by climate change.

According to DOD OIG, DOD's "Adapting to Climate Change, Accelerating Resilience, and Protecting the Environment" addresses three lines of effort of the DOD's Climate Adaptation Plan: making climate informed decisions, training and equipping a climate ready force, and building resilient installations and infrastructure. Key to this challenge is expanding climate literacy and training, integrating climate effects into operations, and addressing installations' maintenance and improvement backlog. DOD has identified climate change as a major national security issue that will increase operational demands, degrade installation and infrastructure resilience, create health risks, and require changes in plans and equipment. DOD is already feeling the effects of climate change, with increasing intensity and frequency of hurricanes, wildfires, floods, and droughts impacting DOD facilities. At the same time, the effects of DOD operations can harm the environment and the health and safety of DOD and non DOD personnel, as evidenced by fuel leaks at the Red Hill Bulk Fuel Storage Facility at Joint Base Pearl Harbor Hickam, Hawaii, and the presence of perfluoroalkoxy and polyfluoroalkyl substances, commonly called PFAS chemicals, in groundwater around military installations.

According to DOI OIG, DOI faces challenges in effectively and efficiently implementing its policies that confront the effects of climate change on its mission, programs, operations, and personnel.

The Fourth National Climate Assessment states that climate change is causing potentially harmful effects on marine and other animal life, increased high temperature extremes and heavy precipitation events, warming and rising seas, more frequent flooding, and increasing wildfires. Natural disasters can expose Federal real property assets—including office buildings, levees, roads, and bridges—to physical damage that can require substantial resources to repair or rebuild.

According to the National Oceanic and Atmospheric Administration, climate change is a contributing factor to increasing extreme weather that leads to potentially multibillion-dollar disasters. In 2021, the United States experienced 20 separate weather and climate disasters where overall damages reached or exceeded $1 billion. Moreover, as the Farm Credit System becomes more complex, FCA will face challenges to address evolving risks, threats, and conditions. The Farm Credit System continues to be impacted by changes in the supply chain, labor market, interest rates, cybersecurity threats, the collective farm debt, and climate.

Appendix: 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, 74 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 74 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 actions. 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 descriptions 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 are required to 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. 5a U.S.C. (United States Code) § 5(d) 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.

Abbreviations and Acronyms

ARPA	American Rescue Plan Act
BOP	Federal Bureau of Prisons
CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CDBG	Community Development Block Grant
CFTC	Commodity Futures Trading Commission
CIGIE	Council of the Inspectors General on Integrity and Efficiency
COPS	Office of Community Oriented Policing Services
COVID-19	Coronavirus Disease 2019
CPSC	Consumer Product Safety Commission
DATA Act	Digital Accountability and Transparency Act of 2014
DEIA	Diversity, Equity, Inclusion, and Accessibility
DFC	U.S. International Development Finance Corporation
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DOD	Department of Defense
DOI	Department of the Interior
DOJ	Department of Justice
DOL	Department of Labor
DOS	Department of State
DOT	Department of Transportation
Treasury	Department of the Treasury
EAC	Election Assistance Commission
ED	Department of Education
ERM	Enterprise Risk Management
EXIM	Export Import Bank
FAA	Federal Aviation Administration
FAR	Federal Acquisition Regulation
FCA	Farm Credit Administration

FDIC	Federal Deposit Insurance Corporation
FEHBP	Federal Employee Health Benefits Program
FEMA	Federal Emergency Management Agency
FIS	Financial Information System
FY	Fiscal Year
GAO	Government Accountability Office
GSA	General Services Administration
HHS	Department of Health and Human Services
HUD	Department of Housing and Urban Development
IG	Inspector General
IRS	Internal Revenue Service
IT	Information Technology
NASA	National Aeronautics and Space Administration
NARA	National Archives and Records Administration
NRC	Nuclear Regulatory Commission
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PIIA	Payment Integrity Information Act
PPP	Paycheck Protection Program
SBA	Small Business Administration
SSA	Social Security Administration
STEM	Science, Technology, Engineering, and Math
TIP	Trafficking in Persons
USAID	U.S. Agency for International Development
USPS	United States Postal Service
VA	Department of Veterans Affairs
ZTA	Zero Trust Architecture

COUNCIL OF THE INSPECTORS GENERAL ★ ON INTEGRITY AND EFFICIENCY ★