Be Better Prepared for the Next Crisis

Through Robust Enterprise and Fraud Risk Management

By Andrew C. Lewis, Kayla M. Futch and Jeffrey C. Steinhoff

By their nature, federal disaster response programs are highly susceptible to fraud, waste and abuse. COVID-19 programs, the nation's largest-ever relief response at $4.6 trillion,[1] were no exception. The government immediately stepped in, disbursing trillions of dollars. Widespread reports of fraud immediately followed, involving tens of billions of dollars.[2] Addressing urgent public needs must always be foremost, and COVID-19 programs were crucial to our nation's wellbeing. However, better safeguarding of assets from fraud is also important.

Recognizing the inevitability of future crises, enhanced planning, capacity building and applying lessons learned are essential to meet urgent needs yet better protect assets when the door to benefits suddenly opens wide. Fraudsters are fully prepared. Government must likewise be ready. Robust fraud risk management (FRM), as an integral part of enterprise risk management (ERM), lays the foundation. Since federal legislation requires both ERM and FRM, extensive standards, requirements, tools and leading practices exist for their application; but they call for greater management attention and accountability. Since fraud risks intensify in a crisis, prioritization of ERM and FRM is crucial to make sure governments use response funds as expected to achieve the outcomes intended.

Fraudsters Are Ready, Willing, and Able When Crisis Hits

Fraudsters follow money and opportunity, which government offers, especially in a crisis. Even when agencies are on alert, based on experience, fraudsters are better prepared. They quickly pinpoint vulnerabilities and know that:

- Normal procedures to prevent fraud are secondary to helping people in urgent need.
- Expediting relief payments and procurement of lifesaving goods and services may bypass normal processes and controls.
- Antiquated systems and processes that lack integration and basic controls may be used to disburse expedited payments.
- New programs may be created on the fly to meet urgent needs, such as the Paycheck Protection Program (PPP), which fraudsters immediately attacked.
- Benefits are not denied when applicants cannot produce eligibility documentation destroyed during a disaster, and self-certification or the honor system can generate initial payments.

This story is replayed during each crisis as fraud perpetrators lie in wait for these situations. Subsequently detecting and recovering fraudulent payments is most often futile.

The Lines Between Fraud, Waste, and Abuse Can Be Blurry

Federal agencies reported a record $277 billion[3] (7% of annual spending) in improper payments for fiscal year (FY) 2021.[4] An improper payment is defined by the Office of Management and Budget (OMB) as one which is "made in an incorrect amount under statutory, contractual, administrative, or other legally applicable requirements."[5] In addition, the Government Accountability Office (GAO) reported that "the government still doesn't fully understand the size of federal improper payments, partly because it doesn't have complete, reliable, or accurate estimates." GAO also noted improper payments related to COVID-19 funding, such as PPP disbursements, were not included in the $277 billion.[6]

Most improper payments represent waste or abuse, but fraud can be appreciable through identity theft and other illicit means. As defined by GAO:[7]

Fraud "involves obtaining something of value through willful misrepresentation."

Waste is "the act of using or expending resources carelessly, extravagantly, or to no purpose." It is primarily caused by mismanagement, inappropriate actions, and inadequate oversight.

Abuse is a "behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary operational practice given the facts and circumstances. This includes the misuse of authority or position for personal gain or for the benefit of another."

These three concepts are intertwined. The only difference may be how a problem is addressed legally, such as settling with the government without admitting wrongdoing for what could arguably be considered fraud. Also, when root causes remain unidentified, what initially appears to be waste or abuse may be fraud. For example, purchasing unneeded, overpriced, or substandard goods and services, while clearly wasteful, could also involve bribery of government officials. The public may not differentiate between them nor care how or why assets were not protected. The problem is that payments flagged as "improper" made headlines, became part of the COVID-19 legacy, and contributed to already low public confidence in government.[8]

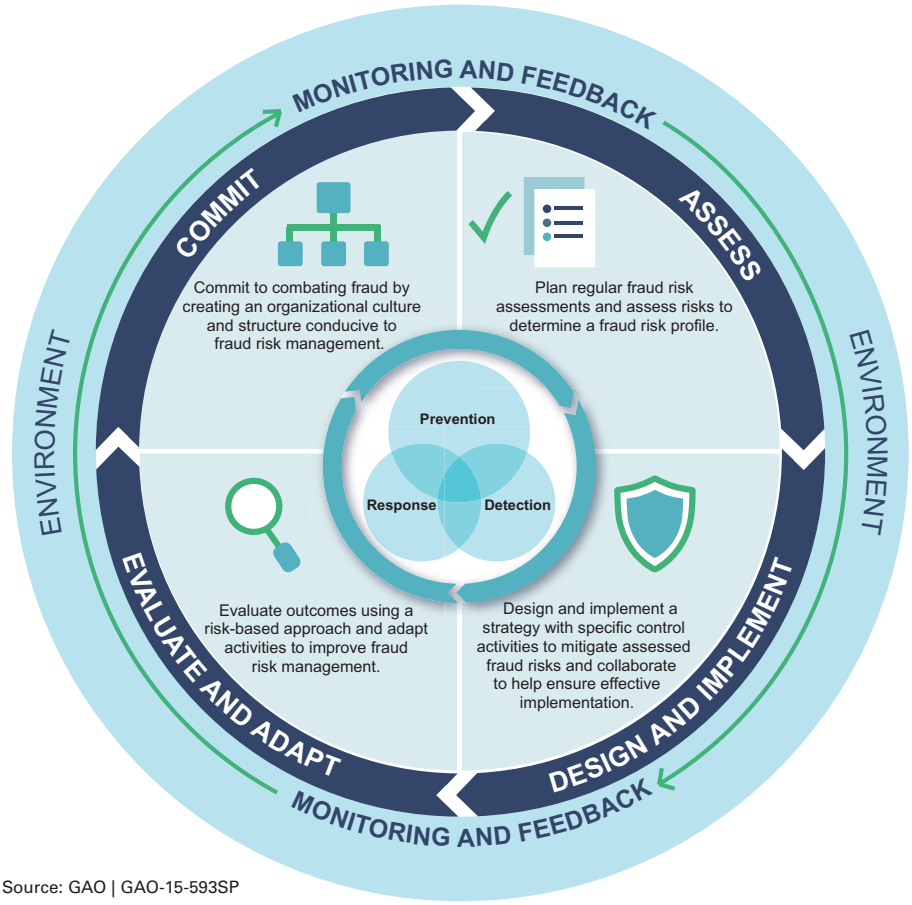
Legislation, Standards, and Guidance Provide a Clear Path to ERM and FRM

ERM and FRM are etched in legislation and implementing standards, regulations, and guidance. Continuing shortfalls point to the need to strengthen agency implementation and accountability for results.[9] As the first line of defense, program managers must fully understand the context of risk management and their roles and responsibilities. The requirements must be viewed as essential to sound program management, not burdensome, "check-the-box" exercises best left to financial managers and auditors.

Concerned with growing reports of fraud, waste and abuse, in 1982 Congress enacted the Federal Managers' Financial Integrity Act (FMFIA).[10] Issued pursuant to FMFIA and, therefore, having the force of law, GAO published *Standards for Internal Control in the Federal Government* and OMB released implementing requirements in Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*. Circular A-123 emphasizes "the need to integrate and coordinate risk management and internal control into existing business activities and as an integral part of managing an Agency."[11]

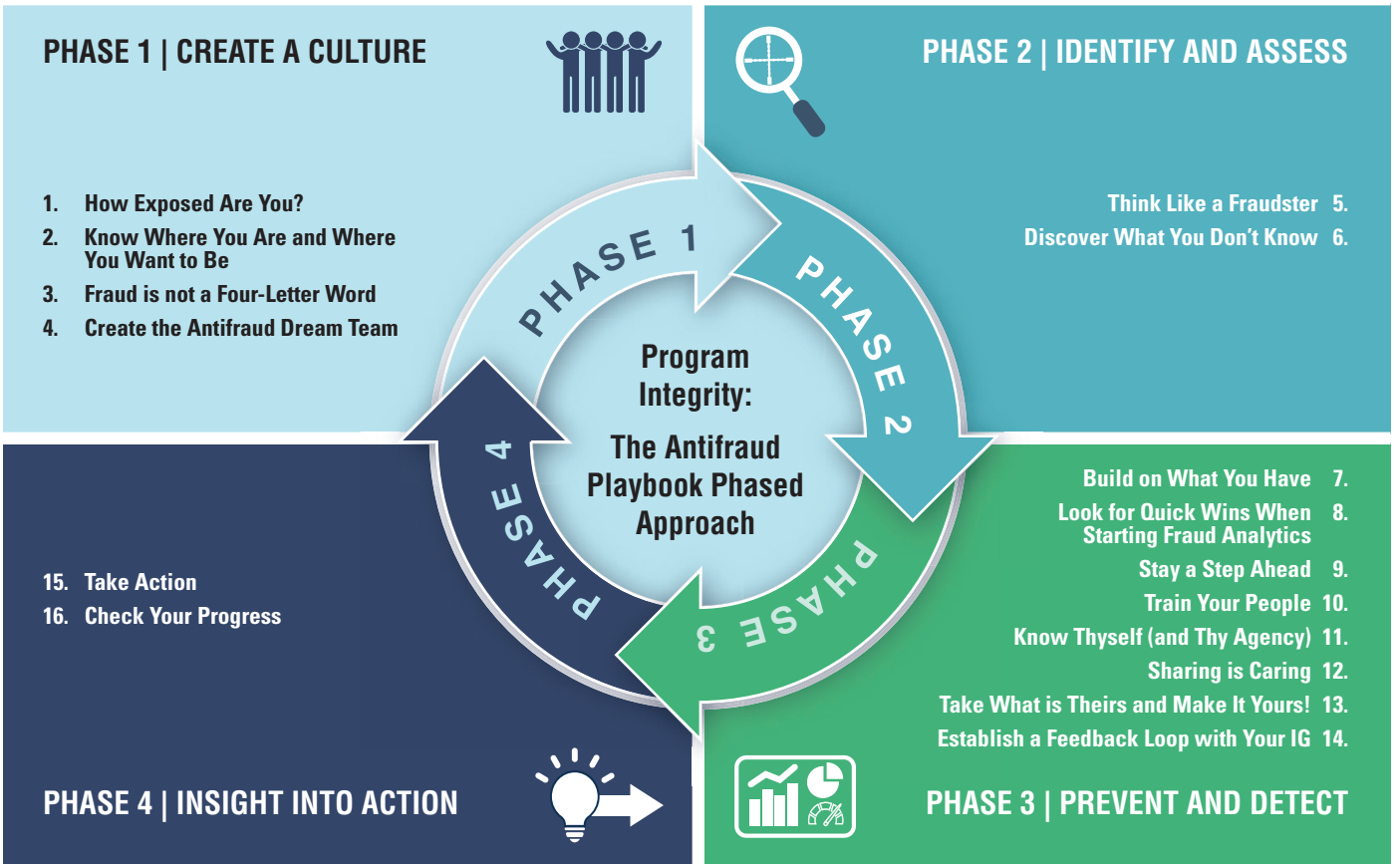
In 2015, GAO published *A Framework for Managing Fraud Risks in Federal Programs*,[12] which organized leading practices into control activities to prevent, detect and respond to fraud. Emphasizing prevention, it includes structures and environmental factors that influence or help managers mitigate fraud risks. The framework also highlights the importance of monitoring and incorporating feedback throughout all four of its components, as shown in **Figure 1**.[13]

Figure 1. GAO's Fraud Risk Framework



Source: GAO | GAO-15-593SP

Figure 2. Playbook Phases and Plays



Source: CFO Council

OMB Circular A-123 requires agencies to adhere to the framework's leading practices as they evaluate internal control and fraud risks with a risk-based approach to identify and mitigate weaknesses. Circular A-123 examines FRM in disaster programs and includes illustrative examples of fraud risk profiles. In 2016, Congress required adherence to GAO's Framework and OMB Circular A-123 through the Fraud Reduction and Data Analytics Act,[14] which was replaced in 2020 by the Program Integrity and Information Act.[15] Congress requires agencies to:

1. Use a risk-based approach to design and implement control activities to mitigate identified fraud risks.
2. Collect and analyze data on detected fraud to monitor trends and continuously strengthen fraud prevention.
3. Use the results of monitoring, evaluation, audits and investigations to improve fraud prevention, detection and response.

In October 2018, the CFO Council (CFOC) and the Department of the Treasury (Treasury) Bureau of the Fiscal Service issued the *Program Integrity: The Antifraud Playbook*, which observes:

> *"You can invest years in building your agency's reputation and public trust in it, and one incident of fraud can destroy it. The American people expect agencies to protect their tax dollars by developing and maintaining governance structures, controls, and processes to safeguard resources and assets. By making the management of fraud risk a priority at your agency, you can balance the achievement of your agency's mission with enhanced program integrity."*

Figure 2 highlights the Playbook's four phases and 16 plays.

In January 2022, GAO launched an antifraud resource website, "Understand and Combat Federal Fraud,"[16] which presents a conceptual fraud model to promote collective understanding of fraud affecting federal agencies. The model systematically organizes key characteristics of fraud schemes, fraudsters, activities, mechanisms and impacts, and it demonstrates the full complexity of fraud relationships through interactive graphics that illustrate fraud concepts. The common framework and vocabulary used to describe and classify fraud events can enhance data analytics, while a graphic user interface supports wide user access.

What Needs to Happen Now?

As OMB Circular A-123 observed, "implementing FRM programs, in tandem with ERM concepts, represents not only significant operational change in many governments but

also, and perhaps more importantly, cultural transformation." Here are 10 interrelated actions based on lessons learned and leading practices that can drive needed transformation.

1. **Hold program managers accountable for ERM and FRM.** While CFOs and auditors must continue to perform crucial roles, program managers must own risk management. Remember: *The Antifraud Playbook* was developed by the CFOC and Treasury, not program managers responsible for following the statutory path. When all embrace congressional intent and make use of the range of available tools, the result is greater understanding, clear expectations, accountability and less fraud. Agencies may need to mandate additional training for program managers to provide context for ERM and FRM and their role in improving program performance.

2. **Use ERM and FRM to address the present and the future.** Leading organizations determine the nature of current and future risks and which risk environment changes are imminent or likely. For example, the Defense Department does not prepare to re-fight previous wars but for future conflicts and aims to remain well ahead of adversaries and threats. Consider what could happen if your agency were suddenly responsible for a large new program that had to be implemented immediately, as occurred during COVID-19.[17] Readiness for the next crisis is possible through strong ERM and FRM programs.

3. **Prioritize risk preparedness.** Strong operational planning, adoption of leading practices, capacity building, timely risk mitigation, and end-to-end testing are essential to preparedness. Once crisis hits, it is too late. So, think like a fraudster! Perform tabletop exercises that simulate fraud attacks to test vulnerabilities across the entire system, including state and local governments that administer federal programs. Identify strong and weak links and establish proper balance between meeting expectations and safeguarding assets. Never again should this nation disburse billions of dollars in taxpayer money to incarcerated individuals[18] and to non-existent businesses, both long-standing problems in relief programs, including ones set up for COVID-19.

4. **Continually measure the impact of relief spending.** Make sure relief funds are being used as expected and achieving intended outcomes by developing metrics and processes to continually track impacts on recipients and the economy. Spending data is one piece of the puzzle but knowing what happened in each relief category is equally crucial. Consider additional aggregation across programs of what recipients did with relief payments identified by demographic group and sector. Find out whether people and businesses that did not suffer losses in COVID-19 were receiving payments, because they were eligible under initial criteria, which was quickly formulated at the outset. There are indications that many saved it for a rainy day as the Federal Reserve reported $4.7 trillion of increased deposits in commercial banks during 2020 and 2021. Were relief funds spent on non-essential products and services? This information would help in assessing whether mid-course eligibility corrections are warranted or in setting eligibility criteria in future crises.[19]

5. **Never allow weaknesses to linger**, or you will pay the price repeatedly. Fraudsters prey on antiquated systems and known vulnerabilities. Addressing identity theft and modernizing systems should be a national priority in partnership with state and local governments and the private and nonprofit sectors.[20] State unemployment insurance (UI) systems were not integrated, and many were antiquated. One COVID-19 fraudster reportedly collected UI from 29 states.[21] Tens of billions of UI dollars lost to fraud during COVID-19 dwarfed the potential cost of developing a modern nationwide, integrated system. Also, as of Nov. 1, 2022, nearly 23,000 GAO and inspector general recommendations remained open — half of them from one to five years and another 12% for more than five years. It's time to address them and relentlessly apply lessons learned.

6. **Reduce fragmentation, duplication, and overlap.** Annually, GAO reports on opportunities to reduce fragmentation, overlap and duplication, citing about $552 billion in savings in 2011–2021. Its May 2022 report identifies actions that could save even more. For example, the Department of Health and Human Services could save hundreds of millions by reducing payments to skilled nursing facilities with high rates of potentially preventable hospital readmissions and emergency room visits. Also, federal contract officials could save billions annually by using metrics to measure cost reduction.[22] Additional focus on fragmentation, duplication and overlap could help mitigate vulnerability to schemes in which fraudsters attack related programs to claim duplicative benefits. By eliminating disjointed structures and fostering governmentwide partnerships, programs can better exchange information to screen recipients.

7. **Make the fraud oversight body established to oversee the government's COVID-19 response permanent.** The Coronavirus Aid, Relief, and Economic Security (CARES) Act set up the Pandemic Response Accountability Committee (PRAC), patterned after the successful Recovery Accountability and Transparency Board established in 2009 under the American Recovery and Reinvestment Act.[23] Through aggressive, continuous auditor fraud oversight and involvement, PRAC galvanized partnerships within all levels of government auditing, serving as auditor, investigator, analyst, advisor, innovator, organizer and facilitator. It has already identified tens of billions of dollars of fraud and initiated recoveries and criminal prosecution. PRAC Chair

Michael Horowitz said it would not surprise him if COVID-19 fraud exceeded $100 billion.[24] Since, the PRAC's mission is limited to the COVID-19 response, government leaders should consider:

- Making the program permanent.
- Expanding its mission to a new governmentwide audit innovation and fraud resource center to synchronize fraud oversight strategies and develop cutting-edge FRM tools and oversight mechanisms.
- Increasing its capacity as a shared resource and a repository of leading government fraud audit and investigative practices.

8 **Aggressively build on the chief risk officer (CRO) concept.** Agency CROs champion ERM and FRM and, from their seat at the table with agency top management, promote a strategically aligned portfolio view of risks, a risk appetite and a fraud maturity model. According to OMB, an effective CRO "develops, manages, coordinates and oversees a comprehensive system for proactively identifying, prioritizing, monitoring and communicating an organization's enterprise-wide risks."[25]

9 **Strengthen cybersecurity.** Cybercriminals, among the nation's highest national security threats, have changed FRM. They come from anywhere in the world, hit quickly, and disappear. GAO first listed information security as a high-risk in 1997. In its 2022 *High-Risk Series* report, GAO noted "risks to IT systems … are increasing, including insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, and the emergence of new and more destructive attacks."[26]

10 **Establish robust fraud risk maturity models.** FRM and ERM are never-ending programs to build capacity and understand strengths and weaknesses for continuous improvement. Input from the inspector general, access to risk management experts, and scorecards that measure maturity are vital. Among the essential maturity areas identified in OMB Circular A-123 are:

- Leadership.
- Risk culture.
- Ethics.
- Risk strategy and governance.
- Risk assessment and measurement.
- Risk management and monitoring.
- Risk reporting and insight.
- Data and technology.

Final Thoughts

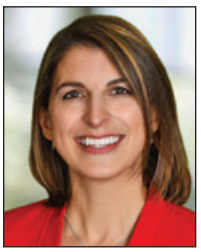
Fraud in government programs steals resources from intended recipients and casts government in a most negative light. A strong framework of legislation, standards, requirements, and tools exists, but its components must be used to their fullest benefit. Take the proactive road that views ERM and FRM as fundamental and valuable program management responsibilities. Break the cycle of recurrent fraud. As PRAC Chair Michael Horowitz said, "You can't have a system where crime pays. It undercuts the entire system of justice. It undercuts people's faith in these programs, in their government. You can't have that."[27] Make ERM and FRM priorities by holding managers accountable and rejecting a compliance mindset. And restore public confidence that government can safeguard assets while achieving intended outcomes! J

Endnotes

1. USAspending.gov, Aug. 31, 2022: Total budgetary resources $4.6 trillion; total obligations $4.4 trillion; total outlays $4 trillion (COVID Relief Spending | USAspending).
2. PRAC (About Us | Pandemic Oversight).
3. An additional $4.4 billion in payments were reported as "unknown" as to whether they were proper payments, bringing the total that was improper and unknown to $281.4 billion, or 7.2% of all FY 2021 payments.
4. PaymentAccuracy.gov (FY2021 Payment Accuracy Dataset_3_14_2022.xlsx (live.com)).
5. OMB Circular A-123, Appendix C, *Requirements for Improper Payment Improvement*, M-21-19, March 5, 2022.
6. GAO. "Improper Payments; Issue Summary" (Improper Payments | U.S. GAO).
7. GAO. *Standards of Internal Control in the Federal Government*, GAO-14-704G, Sep. 10, 2014.
8. Pew Research Center, *U.S. Politics & Policy*. "Public Trust in Government: 1958 to 2022," June 6, 2022.
9. Steinberg, Hal. "Achieving Governmentwide Enterprise Risk Management," AGA *Journal*, Winter 2021.
10. Public Law (P.L.) 97-255, Sep. 8, 1982.
11. 2016 *Playbook: Enterprise Risk Management for the U.S. Federal Government*, developed by the CFO Council and the Performance Improvement Council to bolster OMB Circular A-123, provides leading ERM implementation practices.
12. GAO-15-593SP, July 28, 2015.
13. Ibid.
14. P.L. 114-186, June 30, 2016.
15. P.L. 116-117, March 2, 2020.
16. GAO Antifraud Website (Antifraud Resource (gaoinnovations.gov)).
17. Lewis, Andrew, Nikki Reid and Jeffrey Steinhoff. "Supporting the Nation's War Against Covid-19 Through Accountability, Transparency and Oversight," AGA *Journal*, Fall 2020.
18. In 2005 and 2006, relief payments for Hurricanes Katrina and Rita went to incarcerated individuals, as did UI payments during COVID-19. (GAO. "Hurricanes Katrina and Rita: Improper and Potential Fraudulent Individual Assistance Payments Estimated to Be Between $600 Million and $1.4 Billion," GAO-06-844T, June 14, 2006; and California State Auditor. "Employment Development Department: Significant Weaknesses in EDD's Approach to Fraud Prevention Have Led to Billions of Dollars in Improper Benefit Payments," Report 2020-628.2, Jan. 21, 2021.)
19. Lewis, Andrew, Marlon Perry and Jeffrey Steinhoff. "Will COVID-19 Be a Tipping Point Toward Long-term Fiscal Sustainability," AGA *Journal*, Fall 2022.
20. The National Association of State Workforce Agencies and its UI Integrity Center called identity theft the biggest challenge for states in combating UI fraud. The Labor Department reported that UI payment errors more than doubled in FY 2021 to $78.1 billion. On June 7, 2022, GAO designated the UI system as High-Risk due to "long-standing challenges in meeting the needs of unemployed workers and mitigating financial loss, which worsened during the COVID-19 pandemic."
21. Fahrenthold, David. "Prosecutors Struggle to Catch Up to a Tidal Wave of Pandemic Fraud," *The New York Times*, Published Aug. 16, 2022, updated Aug. 18, 2022.
22. GAO. "2022 Annual Report: Additional Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve Billions of Dollars in Financial Benefits," GAO-22-105301, May 11, 2022.
23. See Endnote 12.
24. See Endnote 21.
25. OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, section 270.24 to 270.29.
26. GAO. "High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas," GAO-21-119SP, March 2, 2021.
27. See Endnote 21.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. This article represents the views of the authors only, and not necessarily the views or professional advice of KPMG LLP.

Andrew C. Lewis, CGFM, CPA, PMP, CIPP/G, is AGA's Past National Treasurer, past co-chair of AGA's Leadership Development Committee, and a member of AGA's Montgomery/Prince George's County Chapter. He is the partner-in-charge of KPMG LLP's federal audit practice, and an executive fellow of the KPMG Government Institute.



Kayla M. Futch, CGFM, CPA, is a managing director in the federal audit practice. She has over 15 years of federal accounting and audit experience and recently served on rotation in KPMG LLP's Department of Professional Practice, providing technical audit and accounting support and guidance to KPMG LLP professionals and clients. She is a member of AGA's Washington D.C. Chapter.

Jeffrey C. Steinhoff, CGFM, CPA, CFE, CGMA, is a senior advisor to KPMG and retired managing director of its Government Institute. He enjoyed a 40-year federal career in which he served as Assistant Comptroller General of the U.S. for Accounting and Information Management, led GAO's largest audit unit, had responsibility for developing government auditing and internal control standards, and was a principal architect of the CFO Act. Jeff is an AGA Past National President, founded the CGFM program, and received the organization's highest honor, the Robert W. King Memorial Award; the Comptroller General's Award, GAO's highest honor; and AICPA's Outstanding CPA in the Federal Government. Jeff is a member of AGA's Northern Virginia and Washington D.C. Chapters and an elected Fellow of the National Academy of Public Administration.