2019 ERM WORKSHOP

Beyond Compliance, Driving Organizational Value

April 11, 2019

AGA®

AFERM
Association for Federal
Enterprise Risk Management

ACKNOWLEDGEMENTS

AGA

Ann M. Ebberts, MS, PMP, Chief Executive Officer

Susan Fritzlen, Chief Operating Officer

Lyndsay McKeown, Senior Manager, Marketing & Design

Mary Margaret Yodzis, Editor

AFERM

Tom Brandt, President

Thomas Holland, Programs Committee Chair

In Appreciation

Special thanks to the Planning Committee who made the workshop possible and to all of the sponsors for facilitating and capturing the round-table discussions from which this report was produced. Additional thanks for the writing of this executive summary to the following contributors:

Sarah Choi, Guidehouse
Thomas Holland, Guidehouse
Bert Nuehring, Crowe
Marianne Roth, Consumer Financial Protection Bureau

AGA is *the* member organization for financial professionals supporting government. We lead and encourage change that benefits our field and all citizens. Our networking events, professional certification, publications and ongoing education help members build their skills and advance their careers.

AFERM is the only professional association solely dedicated to the advancement of enterprise risk management (ERM) in the federal government through thought leadership, education and collaboration. AFERM provides programs and education about benefits, tools and leading practices of federal ERM and collaborates with other organizations and stakeholders to encourage the establishment of ERM in federal departments and agencies.

Executive Summary

On April 11, 2019, AGA and AFERM held their third annual enterprise risk management (ERM) workshop with federal government professionals. The event provided an opportunity for more than 160 individuals to hear the opinions of senior government leaders as well as accounts of their ERM successes and challenges. The participants were also able to discuss and share their agency practices with colleagues concerning ways ERM can, and does, drive organizational value and enhance performance.

The workshop focused on three key areas:

1. Adding Value Beyond the Implementation of ERM: ERM Approaches to Managing Cyber Risks
2. OMB Circular A-123, Appendix A – Far More Than Financial Statements
3. Risk: Part of Your Organization's Culture

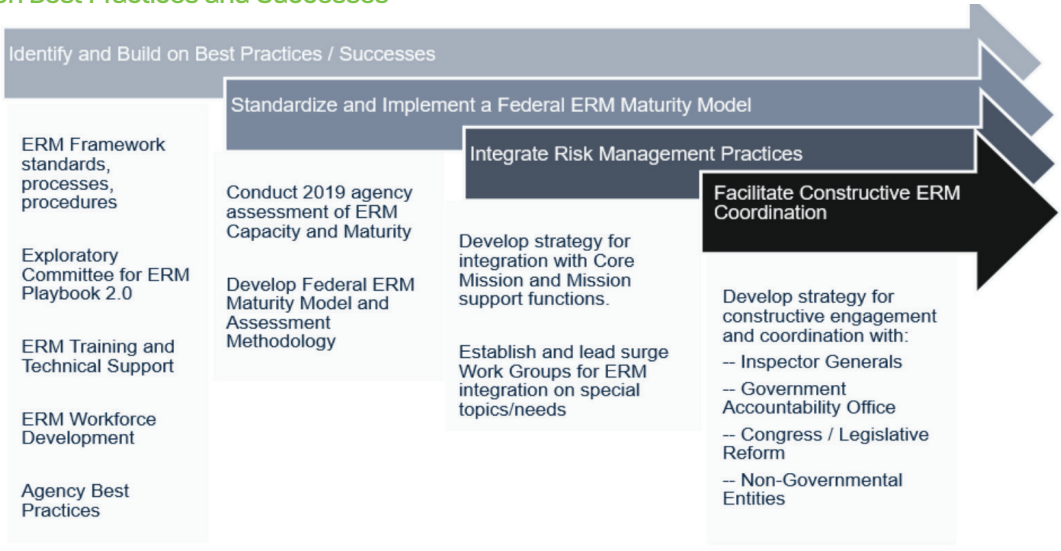
Kicking off the workshop from the Office of Management and Budget (OMB) were Adam Lipton, performance manager in the Office of Performance and Personnel Management; and Dan Kaneshiro, a policy analyst in the Office of Federal Financial Management. The two spoke on the establishment of a cross-agency executive steering committee focused on ERM as well as a committee to explore whether to update the ERM Playbook (the Playbook). They identified OMB strategies and priority efforts for moving forward with ERM, using the below chart **(Figure 1)**.

The structure of the daylong workshop included short, focused presentations on each of the three key areas listed above.

1. In the first session, Peter Gouldmann, enterprise risk officer for cyber at the U.S. Department of State, discussed ways cyber risk management and ERM can support one another. He also shared insights on applying concepts traditionally associated with ERM for better cyber risk management.
2. In the second session, Phillip Juengst, director of the internal controls division of the U.S. Department of Education (DOE), and Michael Wetklow, deputy CFO of the National Science Foundation (NSF), spoke on the updated OMB Circular A-123, Appendix A, and what their respective agencies are doing to implement it.
3. In the third session, John Basso, deputy assistant secretary for planning and performance management at the U.S. Department of Veterans Affairs (VA), and Montrice Yakimov, chief risk officer of the Bureau of the Fiscal Service (Fiscal Service), shared their perspectives on ways to embed good risk management and ERM practices into an organization's culture.

Facilitated small group discussions followed each presentation. At each of 16 tables, participants shared knowledge, experiences, ideas, and best practices on the topic just presented. This report captures many of the ideas and innovative practices identified during these discussions to allow AGA and AFERM to share them with the wider federal ERM community.

Figure 1: Identify and Build on Best Practices and Successes



Session 1: Adding Value Beyond the Implementation of ERM: ERM Approaches to Managing Cyber Risks

There are no guarantees in cybersecurity. In this session, Peter Gouldmann of the State Department shared his views on ERM approaches to managing cyber risks. He said advanced persistent threats, zero-day threats, and thousands of attacks per day make it impossible to eliminate cyber risks. For this reason, although fundamental tenets of ERM are important regardless of the topic, ERM is invaluable in managing these risks.

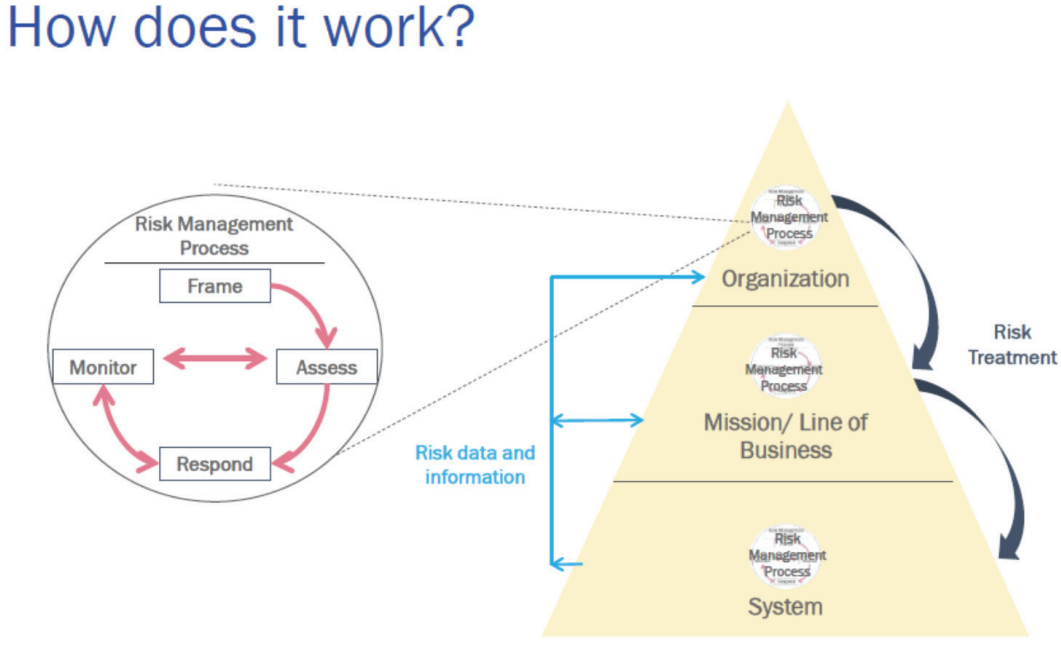
Cyber risk information was around long before ERM gained widespread interest in the federal government, but ERM implementation has lagged. As agencies execute and mature ERM programs, integrating cybersecurity as a mainstream function will strengthen the risk posture of an organization. An ERM approach will help ensure cyber risks are translated at each organizational tier. If a system risk and a business or mission function rely on the system functions, then the risk information must be communicated in a meaningful way to each level of the organization. Appropriate conversations must then be held to determine what this risk means and what steps to take. (Figure 2)

Translation of risk going up the management chain is as vital as the translation of the required response going down to all involved. Critical to ensuring this communication process is working is to know your agency business processes, to characterize your specific threats, and to plan risk treatments to build business resiliency.

ERM and Cybersecurity

Cybersecurity attacks and risks are growing in frequency, significance and impact, thus requiring the ERM framework to capture and manage them. As cyber incidents increase throughout government, alignment with both ERM and crisis management programs is essential. The increasing risks posed by cybersecurity threats present multiple challenges to agencies. According to workshop participants, the first challenge for IT and security professionals is to quantify the

Figure 2



This model enables organizations to frame, assess, respond to, and monitor risks independently at each level – Organizational, Mission, and System.

business impact of cybersecurity events, including agency leadership awareness of the threats the organization faces and identification of the appropriate method for the agency's response. It is very difficult to understand the impact of an event; quantifying the likelihood of such an event is even harder.

Additionally, a disconnect often exists between the terminology used by cybersecurity and ERM programs. Most risks have specific meanings and can be quantifiable to the agency. These quantities can determine the remediation steps necessary to address the risks based on a cost-benefit relationship. However, cyber risks are often unquantifiable to an agency's bottom line, especially if the risk event could potentially jeopardize the agency's reputation.

It is important, then, for information security professionals to provide understandable information to the rest of the organization. Presenting an issue in technology-oriented jargon does not always help convey its impact on business operations. Under such circumstances, agency leaders and information security professionals must communicate about risks to understand their threats to the system before they collaborate to determine the tools needed to manage them. The more information the security professionals can provide to agency leaders about the business impact, the better the opportunities to mitigate cyber vulnerabilities. More knowledge of the bottom-line cost to the organization – whether financially, operationally or reputationally – can help an organization make the most informed decisions on allocating resources to the issue.

Participants added that it is vital for an agency to address risks according to the magnitude of their threats. However, personnel often lack the experience to weigh the significance of a risk to their agency. One solution is to complete a data privacy assessment, which can help an agency better determine where to focus attention and to communicate issues providing direct evidence of their risks. Such assessments have become a crucial tool for incorporating cybersecurity risks into an organization's ERM program to clarify issues and ways to mitigate them.

Several agencies indicated that IT "portfolio" review functions have successfully utilized ERM to understand cybersecurity strategy and to determine investments necessary. Such functions could include review boards to oversee the modernization of the technology, including the investment in cybersecurity technologies.

Many participants said they felt that cyber threat communication and education is important for employees to understand the agency's cybersecurity risks. Many said most training available today in their agencies lacks the emphasis on each individual's responsibility to manage cyber risks. They called for better training and communication to improve employees' understanding of what to look for in their daily activities. They desire more hands-on training plus instruction in recognizing dangerous aspects of cyber risks. In addition, changing the culture of cyber risks from one of fear to one of understanding can help an organization prepare its first line of defense for cyber threats.

Session 2: OMB's Circular A-123, Appendix A – Far More Than Financial Statements

In the second session, Phillip Juengst of DOE and Mike Wetklow of NSF shared their views on the revised OMB Circular A-123, Appendix A, released June 6, 2018. The updated guidance aims to: "(1) effectively manage taxpayer assets, including government data; (2) improve data quality; and (3) reduce burdens on agencies by shifting away from compliance activities and toward actions that will enable the reporting of high quality data in support of data-driven decisions, federal governmentwide management analyses, and transparency." The update provides agency flexibility to determine which control activities are necessary to achieve reasonable assurances over internal controls and processes that support all data quality contained in agency reports. Specifically, the revised appendix:

1. Creates a new requirement that enhances the focus on the Data Accountability and Transparency Act (DATA Act) and requiring a data quality plan
2. Increases the scope from internal control over financial reporting to "internal control over reporting" (i.e., no longer just a financial organization effort)
3. Incorporates ERM
4. Recommends leveraging existing functions within the organization to better monitor and assess risk and improve data quality.

Wetklow also referred to the table shown in Figure 3, identifying how to address the integration of the requirements and intent of the new Federal Data Strategy with ERM programs.

This second small group session at the ERM Workshop focused on the evolution of Appendix A in government agencies and how they are preparing to tackle the requirements of the revised Appendix A.

Evolution of Appendix A

Many agencies have followed the traditional evolution of OMB Circular A-123, Appendix A, and continue to maintain a heavy focus on financial controls. Some participants remarked on the difficulty in getting their agencies to think beyond what they know. Many believe agency financial risks to be well controlled because few issues have arisen and little to no change has occurred in many years. The realization that the same controls continue to be tested every year with the same rigor is shedding light on the value of the Appendix A revision, which requires all reporting to include internal control, not just financial reporting.

At one agency, the materiality level drives control testing and, thus, every high-risk process is tested, locking the agency into the same risks and controls annual testing cycle. To break out of this cycle, participants recommended the use

Figure 3

Internal Control Standard (1)	Common to ERM and Internal Control (1)	Introduced in IC and Expanded in ERM (1)	Incremental to ERM (1)	New Federal Data Strategy (2) Incremental to ERM and IC
Control Environment	Yes	Yes	Yes	TBD
Risk Assessment	Yes	Yes	Yes	TBD
Control Activities	Yes	No	No	TBD
Information and Communication	Yes	Yes	No	TBD
Monitoring	Yes	No	No	TBD

(1) Based on COSO. **(2) Reference: Federal Data Strategy, https://strategy.data.gov**

of ERM practices, such as reviewing and refreshing the risk ranking, to identify areas that may be over-controlled and do not need as much focus as other areas that might be just as risky but are not getting enough management attention. Furthermore, there is an opportunity to ask why certain things are being tested, to force the organization to take an ERM perspective and consider residual risk. If the residual risk is low, what is the value in continuing to test it? Assumptions should be documented, and resources should be redirected to areas that are undermanaged.

Other agencies have begun looking at non-financial controls and involving individuals from the program side in control assessments. Some agencies have acknowledged the need to move away from solely compliance-focused activities and have begun to use data analytics to think about strategy and effectiveness. Others have scaled back control testing and moved toward an entity-level and programmatic controls assessment approach to leverage ERM, add value and inform decision-making.

Other ways that agencies have shifted their Appendix A activities include:

1. Conducting reviews every three years instead of every year
2. Conducting risk assessments or comparing results of risk assessments from year to year to prioritize reviews
3. Simply scaling back compliance exercises. For instance, if a process is in place and no changes have occurred, testing is not required.

Session discussions on the future of Appendix A efforts also included:

1. Using data analytics to identify problem areas
2. Developing risk profiles at the entity level
3. Developing risk registers
4. Performing risk analysis and focusing only on significant risk areas
5. Building and fostering relationships with senior management, the ERM office and the internal controls team
6. Appointing a chief risk officer
7. Developing a culture survey
8. Establishing an incident-reporting policy or ERM playbook.

Given the recent changes in OMB Circular A-123, Appendix A, a vast range of activities support efforts to enable greater coordination and collaboration between ERM and internal controls.

Tackling Data Quality Plan Requirements

One shift in the revised Appendix A requires the development of a data quality plan. Participants shared that their agencies are beginning efforts to build data quality plans and, in some cases, leverage existing cross-agency groups. The focus has been on identifying the right people to perform data quality work. For some agencies, scaling back testing and documenting to a cycle of more than one year – for instance, three years – has made it feasible to take on this additional requirement.

Future of the Workforce

Succession planning and the lack of skilled resources is a risk many agencies identified as a concern. Agencies recognize the need for different skill sets in the future, not only from an analytics perspective but also due to the expansion of Appendix A. Consequently, the workforce is changing to reflect the need for more specialization on the program side. Although a recognized need exists to address these evolving changes, hiring additional staff is not always an option. Various issues, such as limited hiring budgets, lengthy onboarding processes, and insufficient or absent resource selection pools, block improvements.

There is, however, an opportunity to leverage existing agency personnel. The workshop participants discussed the prospect of agency ERM practitioners becoming business consultants for program managers. ERM practitioners are often equipped to work with controls and map them to agency strategic plans. They can be partners in building out control monitoring and connecting internal control teams in areas where they were involved before.

Discussions of the workforce also touched on the way technology creates both risk and opportunity for agencies. Some agencies are exploring blockchain and robotic process automation (RPA). As agencies deploy these technologies, they will begin to replace the repetitive, work efforts and free up staff to handle more meaningful, complex analytical tasks. This transition will result in structural change in the way agencies carry out their work. Additionally, the controls and ERM domains will need to complement data science and data analytics functions. If agencies are not prepared to reskill staff, it may be a missed opportunity.

It is still early in the shift for OMB Circular A-123, Appendix A. Opportunity remains to utilize ERM to support strategic thinking in implementing the requirements of Appendix A to bring value to agencies.

Session 3: Risk: Part of Your Organization's Culture

OMB Circular A-123 and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) ERM Framework articulate the importance of culture to a successful ERM program. Montrice Yakimov, the Fiscal Service's chief risk officer, and John Basso, the VA's deputy assistant secretary for planning and performance management, discussed ways to address culture in ERM programs.

Culture is a key element of COSO's definition of ERM – "the culture, capabilities and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value." The COSO ERM Framework goes on to define culture as the "attitudes, behaviors and understanding about risk, both positive and negative, that influence the decisions of management and personnel and reflect the mission, vision and core values of the organization." In practice, a risk-aware culture is manifested in the ways in which members of an organization – from leadership to front line employees – collectively perceive and respond to risk.

The small group discussion for this session focused primarily on two topics – ERM and culture; and the building and measuring of a risk-aware culture.

ERM and Culture

Participants discussed how an organization's ERM program contributes to building a positive culture in their organizations. A common theme throughout the discussions was the tone at the top and leadership's attitude toward ERM. ERM implementation appeared to be the most successful at agencies where leaders understood the importance of and need for ERM. Setting a positive tone at the top is critical for success because it conveys to all employees that their leadership sees value in ERM. Participants also expressed the importance of implementing ERM-related policies and procedures to "back up" the tone at the top.

In agencies where the tone at the top was indifferent to or unaware of the need for ERM, implementation struggled and ERM practitioners faced an organizational culture that was not conducive to transparency and accountability. In these organizations, unwillingness and fear to reveal "my risks" to others was common. Having risks and transparently communicating about them, to them, carried a negative connotation. The contributing factor seemed to be fear of retribution through reporting or disclosing risks. Some agencies felt they have the "endorsement" of executives to implement ERM, but not the "engagement" to keep the program moving along as it should, to realize the full benefits of ERM.

Building and Sustaining a Risk-Aware Culture

There was a consensus among participants that every agency has an opportunity to shape a positive, risk-aware culture. Participants said they felt ERM programs play an important role in embracing transparency and building trust among employees. They identified six categories of building and sustaining a risk-aware culture, which are listed alphabetically below and include practical examples from the participants.

Communication

Participants indicated that open, transparent, and frequent communication is effective in building trust and buy-in across an organization. Agency newsletters and updates are an effective means of increasing awareness of ERM and reinforcing a risk-aware culture. For example, one agency distributes quarterly newsletters to all employees, highlighting various elements of the ERM program, and then archives them on the agency intranet for easy reference. Others noted that their agency newsletters "formalized" the ERM implementation process and increased ERM awareness and buy-in. Some agencies regularly share updates to their risk profiles through email blasts. Other organizations make their executive-level risk dashboard available to everyone at the agency.

Targeted outreach is another way to build a risk-aware culture. In one agency, the ERM office conducts annual visits to each region and interviews staff to collect feedback on ERM progress and culture. Other participants advised that ERM leaders should create channels of communication and listen to groups that historically are not "at the table" or "in the conversation" when setting agency objectives.

Employee Engagement

Involving employees from different parts of the agency and with varying levels of experience has been significant in building and reinforcing a risk-aware culture. Some agencies found success in creating governance bodies or working groups. One example is an "ERM Council" made up of personnel from different departments who meet regularly to discuss their risks, risk appetite, and the related risk tolerance. Some agencies leverage diverse working groups to assist in conducting risk assessments and monitoring risks. Many participants agreed on the importance of finding ways to encourage people to identify, report, and escalate new or emerging risks. With each of these approaches, participants strongly recommended ERM practitioners provide transparency to staff about the utilization of risk analyses they have conducted.

Less formal employee engagement has also been effective for some agencies. For example, some agencies conduct internal ERM conferences or regular ERM lunchtime learning courses. Fostering an internal network or community of practice of risk professionals is another approach to fostering greater employee engagement.

Incentives and Accountability

Incentivizing employees to demonstrate behaviors consistent with a positive risk culture is a critical component of ERM success. Some ERM programs formally recognize employees who have identified or mitigated risks in their agency. Others focus on communicating to employees that their participation in the ERM process and their feedback is valued.

Enhancing accountability through the individual performance management process is another technique used by some agencies. In these instances, ERM or risk management requirements or goals are added to manager/supervisor or senior executive performance plans.

Leadership Engagement

Many participants discussed the importance of facilitating risk conversations between political leaders and federal career executives. One participant recommended ERM practitioners develop skills in "managing up." Essential is first to understand leaders' perspectives on risk and then discuss how ERM can help leaders achieve their organizational goals. Some participants recommended encouraging leaders to engage in professional programs, such as the Federal Executive Institute, to broaden perspectives on leadership and drive others toward mission achievement.

Organizational Integration

Some agencies found integrating ERM program requirements and concepts into existing agency policies and procedures to be effective. Several participants said their agencies incorporated ERM into their strategic plans. ERM practitioners might work with business units to link their objectives and risks to the enterprise objectives and risks to show staff how each group contributes to the overall organization. Other suggestions included: integrating ERM into the employee onboarding process; embedding risk in strategic initiatives; and linking the risk profile to the GAO High Risk List, if appropriate.

Training/Education

Many participants felt ERM practitioners must educate their workforce on ERM and risk management concepts. Such training highlights the importance and value of effective ERM. Some agencies found targeted training sessions to be the most effective. For example, they developed training for specific audiences, perhaps using more tailored language and applications to address objectives of the audience being trained

Other agencies found embedding ERM or risk management concepts into existing trainings and materials was better. At one agency, ERM instruction takes up one full day of their project management leadership program. At another, they conduct mock risk events to help the workforce learn the importance of risk management at all levels in the organization.

Measuring Risk Culture

Participants also discussed ways their organizations measure risk culture. Some conduct periodic employee surveys with specific questions on risk culture. These organizations have found that following up the survey with focus groups or targeted discussions can be effective in understanding the culture and developing plans to improve it. Other organizations identified the challenges of employee surveys, such as bias or a limited response pool. Some use an ERM maturity model or internal control assessments to help gauge culture.

Participants concluded that ERM practitioners must use a multi-faceted approach to build and sustain a risk-aware culture in their agencies Tone at the top, communication, employee engagement, incentives and accountability, leadership engagement, organizational integration, and training and education are all powerful tools they can use to create and maintain a positive and risk-aware culture.

Conclusion

ERM implementation is well underway across the federal government. This annual workshop from AGA and AFERM provided another opportunity for ERM practitioners to connect and share insights, best practices and ideas with senior government leaders and colleagues.

The workshop touched on key areas that are challenging government organizations and ways ERM can drive real and sustainable organizational value. Workshop participants agreed that integrating ERM practices in managing cyber risks, internal controls and data, and organizational culture is creating opportunities for enhancing agency performance. The workshop discussions provided participants an opportunity to hear how agencies are leveraging ERM in decision-making, enabling more efficient and effective mission delivery.

Appendix: Participating Government Entities

Administrative Office of the United States Courts
Commodities Futures Trading Commission
Consumer Financial Protection Bureau
Defense Intelligence Agency
Environmental Protection Agency
Equal Employment Opportunity Commission
Export Import Bank of the United States
Federal Accounting Standards Advisory Board
Federal Deposit Insurance Corporation
Federal Emergency Management Agency
Federal Energy Regulatory Commission
Federal Housing Finance Agency
Federal Retirement Thrift Investment Board
Food and Drug Administration
General Services Administration
Government Accountability Office
Millennium Challenge Corporation
National Aeronautics and Space Administration
National Archives and Records Administration
National Institute of Standards and Technology
Office of Personnel Management
Pension Benefit Guarantee Corporation
- Office of the Inspector General

Railroad Retirement Board
Securities and Exchange Commission
- Office of the Inspector General

Social Security Administration
Transportation Security Administration
U.S. Census Bureau
U.S. Department of Agriculture
- Food and Nutrition Service
- Rural Development

U.S. Department of Commerce
- National Oceanic and Atmospheric Administration

U.S. Department of Defense
- Department of the Army
- Department of the Navy
- United States Coast Guard

U.S. Department of Education
- Federal Student Aid
- Office of the Inspector General

U.S. Department of Energy
U.S. Department of Health and Human Services
- Office of the Inspector General

U.S. Department of Housing and Urban Development
U.S. Department of Justice
- Bureau of Alcohol, Tobacco, Firearms and Explosives
- Federal Bureau of Investigation

U.S. Department of Labor
- Office of the Inspector General

U.S. Department of State
- Office of the Inspector General

U.S. Department of the Interior
- Fish and Wildlife Service

U.S. Department of the Treasury
- Bureau of the Fiscal Service
- Internal Revenue Service
- Office of the Comptroller of the Currency
- Treasury Inspector General for Tax Administration

U.S. Department of Transportation
- Federal Railroad Administration
- Maritime Administration

U.S. Department of Veterans Affairs
U.S. Patent and Trademark Office

Thank you to our Sponsors

www.agacgfm.org

www.aferm.org