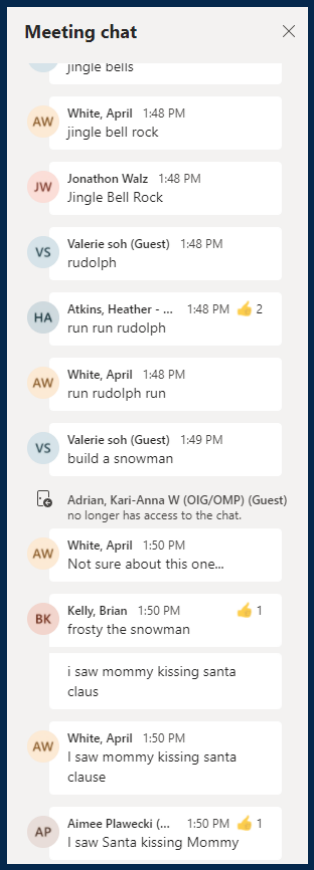
December 2021

ERM Times Newsletter

In this Issue

The latest news and trends in enterprise risk management (ERM) from the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) Enterprise Risk Management Working Group (ERMWG).

Thank you for participating in our last meeting of 2021. We will see you in March 2022!



Wishing you a Joyful Holiday Season!

About ERMWG

CIGIE's ERMWG contributes to the promotion and implementation of ERM principles in accordance with OMB Circular A-123 within the offices of the Inspectors General (OIG) community. For the latest, visit the ERMWG page on the CIGIE website.

2021 AFERM ERM Summit Highlights

The Case for a Federal Chief Risk Officer

Paul Walker discussed Applying Enterprise Risk Management Principles to the U.S. Government


Applying Enterprise Risk Management Principles to the U.S. Government

The coronavirus (COVID-19) pandemic has reminded CPAs that the world is risky, volatile, and uncertain. Some risk experts contend that the world has been this way for a long time. Analysis from the University of Cambridge's Centre for Risk Studies shows that crashes of at least 10% have occurred every 16–17 years for the last 200 years in both U.S. and U.K. markets. The reasons vary, from the cotton crisis and railroad failures in the 19th century to the Great Depression, the OPEC oil embargo, and Black Monday in the 20th century to the dot.com bubble, the global financial crisis, and the COVID-19 pandemic in the 21st century.

What has changed is how enterprises have become more sophisticated at building methods to manage these risks and uncertainties.

The President acts as the de facto "chief risk officer" of the United States. Although previous presidents have taken corrective action to address some of the greatest risks facing the country (e.g., national security and cybersecurity threats, economic downturns, natural disasters), developing an enterprise risk process that aggressively and proactively identifies, prioritizes, and manages risks would be a major step forward.

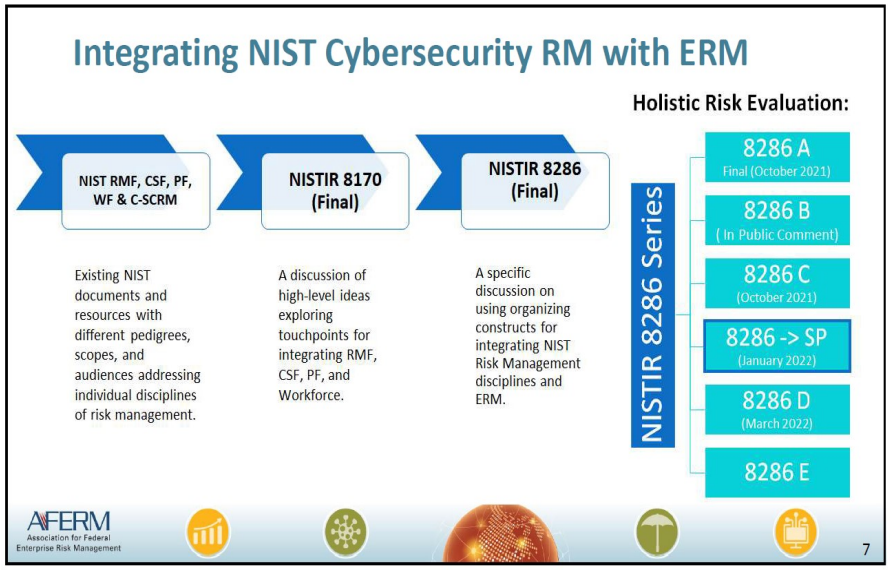
Imagine a Cabinet appointment that oversaw the nation's risk management process, working with Congress, government agencies, corporations, nonprofit organizations, and various thought leaders. Developing an ERM process for the U.S. government would be an approach that:

- Identifies the top risks on a regular basis.
- Manages risks centrally instead of having different agencies manage risks in silos.
- Manages the country's risks proactively rather than taking correcting action after the fact.
- Applies tools, such as scenario analysis, strategic disruption analysis, or pre-mortems to understand how risks would play out.
- Applies advanced metrics (e.g., predictive analytics) using unbiased data, risk-indicating data, and data around impact, likelihood, and velocity.
- Considers impact from a variety of perspectives, as well as how risks are connected, change or create other risks, and how they can be triggered.
- Recognizes the trade-off between position and momentum for dramatically changing conditions (Heisenberg's uncertainty principle applied to risk).
- Understands and factors in the intentions of others (akin to game theory).
- Understands and factors in human cognitive biases and viewpoints.
- Routinely reports on its plans to manage significant risks to its stakeholders.

Presented at the 2021 AFERM ERM Summit

2021 AFERM ERM Summit Highlights

Integrating NIST Cybersecurity Framework into Enterprise Risk Management

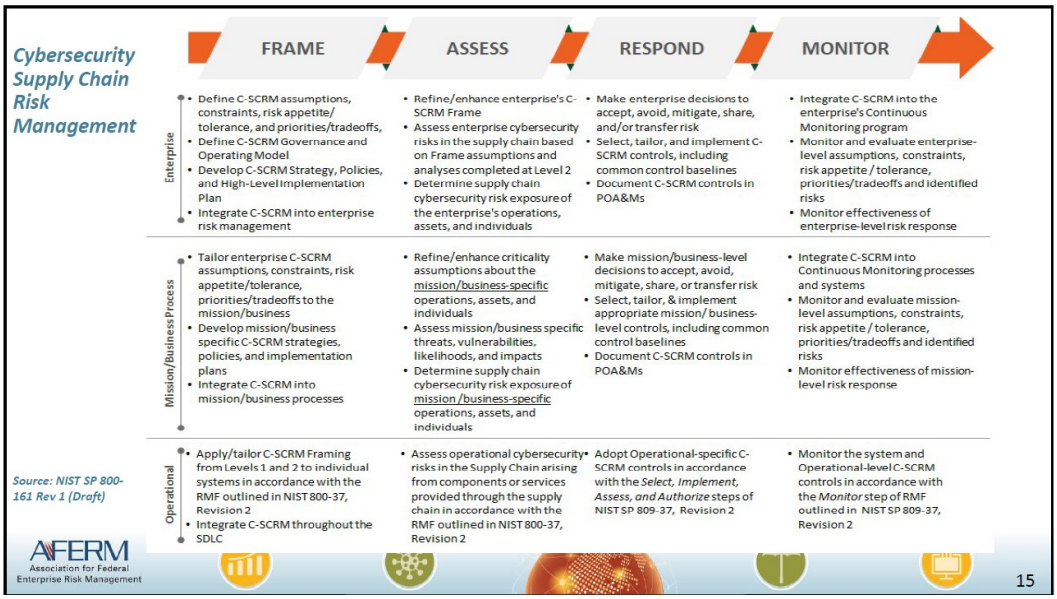


NIST 8286 Series

The increasing and evolving frequency and severity of cybersecurity attacks means that enterprises should ensure that cybersecurity risk is receiving appropriate attention within their ERM programs. NIST 8286 is intended to help with the integration of cybersecurity and ERM.

Cybersecurity Supply Chain Risk Management

After the SolarWinds cybersecurity incident, agencies are assessing their cyber supply chain procedures. NIST 800-161 provides a framework for agencies.



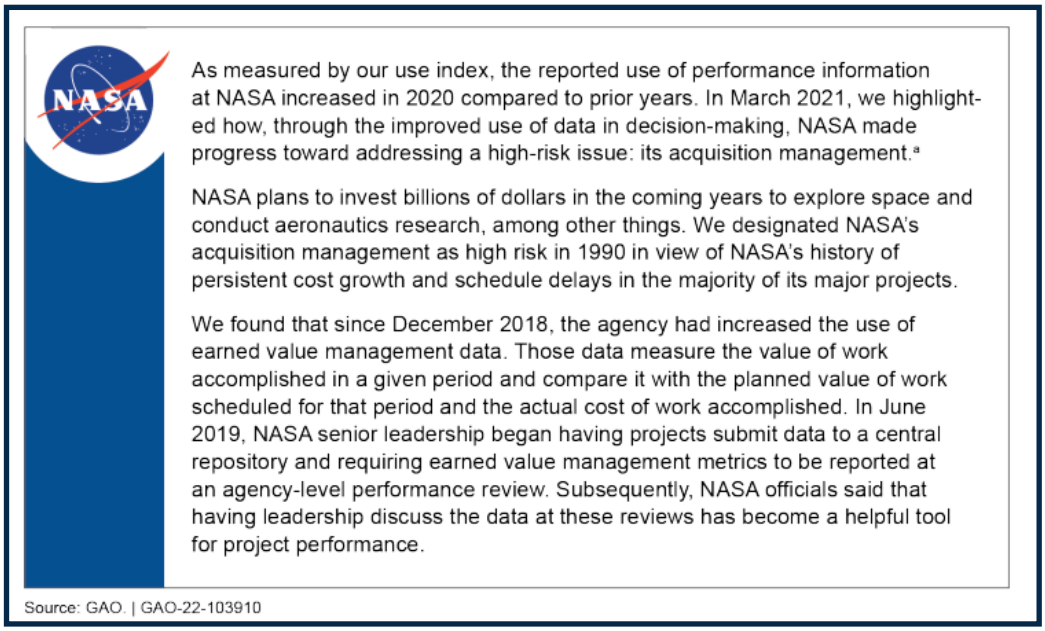
Presented at the 2021 AFERM ERM Summit

GAO Report: Evidence-Based Policymaking

Interested in Evidence-Based Policymaking?

See GAO's latest report on Evidence-Based Policymaking released in November 2021. Per GAO's report, performance information can help decision makers understand and improve results at federal agencies. GAO's 2020 survey of federal managers showed that the reported use of performance information in decision-making generally increased across the federal government.

Prior GAO work highlighted actions that NASA has taken since December 2018 to increase its use of performance information to improve the management of its acquisition projects.



Practices that can Promote the Use of Performance Information:

- Aligning agency-wide goals, objectives, and measures
- Improving usefulness of performance information
- Developing capacity to use performance information
- Demonstrating management commitment
- Communicating performance information frequently and effectively

Read full report at: GAO-22-103910, EVIDENCE-BASED POLICYMAKING: Survey Results Suggest Increased Use of Performance Information across the Federal Government

The GREAT Resignation

Private sector companies might be dealing with a wave of employee resignations, but agency chief human capital officers said that inside the federal government, the situation is different. At least for now.

Instead, chief human capital officers said their agencies are viewing the current moment as an opportunity, a chance for them to become more flexible, attract private sector workers looking for a change and retain current federal employees wanting to keep what they got a taste of during the pandemic.

"I do not think there is a great resignation ahead of us," Traci DiMartini, chief human capital officer at the General Services Administration, said last week at a virtual AFCEA Bethesda event on workforce transformation. "I think there's a great right-sizing ahead of us, particularly in the federal government."

Keith Krut, NASA's chief of people analytics, described the current environment as the "great reevaluation," a period where employees across public and private sectors are reconsidering what they want from their jobs. Employers, including NASA, are trying to quickly respond to their desires.

Wonzie Gardner, the chief human capital officer for the National Science Foundation, said he is seeing some long-time employees retire from his agency. But he said this moment of the "great retooling," where agencies are rethinking what work means. Some are making full-time telework, remote work and other flexibilities permanent.

"This pandemic has been a catalyst for people to make decisions about where and what they want to do with the rest of their lives," Gardner said. "As part of the federal enterprise, I look at it as how do we retool that particular job and be able to pivot to get more of the types of people we want for the 22nd century?"

Immigration and Customs Enforcement is working on its own workplace transformation initiative, one that involves shifting resources from brick-and-mortar facilities to people and technology.

"This is going to be the long-term strategy and plan for the agency, with which we are going to deliver an innovative and adaptable workplace model," said Waldemar Rodriguez, associate director of ICE's Office of Professional Responsibility. "The focus is going to be on mobility, flexibility and mission effectiveness. Coincidentally this fits very nicely with where we find ourselves today, where we've been the past year-and-a-half, and where we think we'll be for the next couple of years. We want to create a workplace for the workforce that focuses on continuous engagement that reaches beyond legacy constraints. We're very tied to physical facilities … but we want to go beyond those constraints to advance the mission by focusing on technology and people."

Read original article: Time for the 'great resignation?' Not for the federal government, CHCOs say | Federal News Network

ERM in the News

The CFO on the Front Lines of Cybersecurity

By: Tony Chiles

ERM, a sweeping discipline and valuable strategic tool, should always be a work in progress. ERM informs cybersecurity decision-making by helping the agency identify vulnerabilities. While ERM encompasses much more than cybersecurity, cyber is a critical component.

Since risk is inherent in financial operations and agency mission delivery operations, and since cybersecurity has grown exponentially in recent years, the CFO and CIO should collaborate to factor financial risk into overall ERM. CFOs can apprise leadership of current and future financial risk for informed decisions about cybersecurity investments. Also, the financial management function as a whole can help identify and mitigate threats by sharing the tools and strategies used in financial data analysis with the cybersecurity team. The CFO's policies, practices, and procedures should filter throughout the agency, not just to financial management professionals. Risk management matters most, in fact, offices that interface with financial systems, often populated by employees unfamiliar with cybersecurity. On the lookout for nascent issues, the financial management team can prevent and report problems for a more paid response to cybersecurity threats and breaches.

Read full article: Journal of Government Financial Management, Summer 2021

Zero Trust in a Virtual Cybersecurity World

By: Tony Hubbard, Joseph Klimavicz, Steve Wong, and Jeffrey Steinhoff

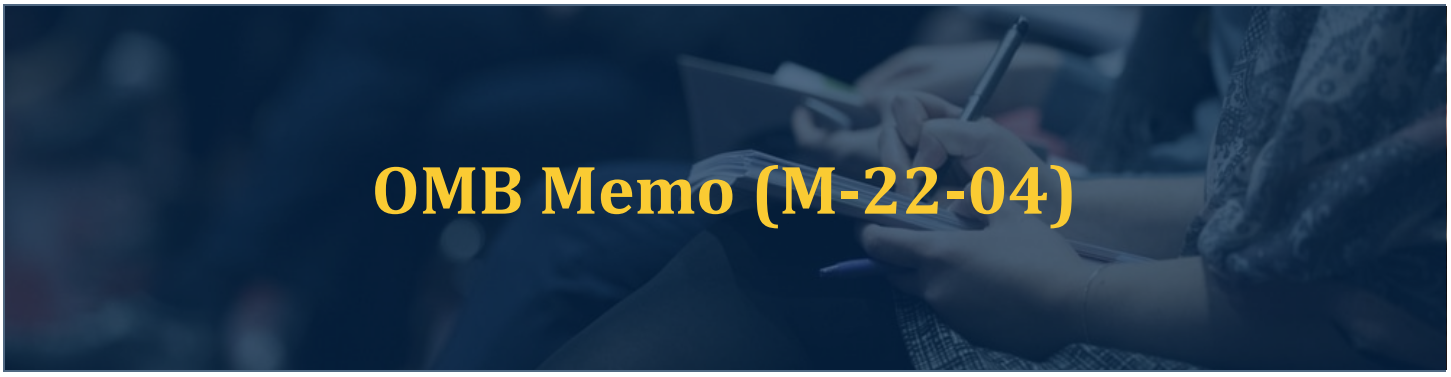
Government IT Remains High Risk

Cybersecurity in a virtual world is dramatically different from defending systems and information within defined perimeters. With the growth of enterprise networks as governments move more data to the cloud and large numbers of personnel work remotely, traditional "perimeter-based" cybersecurity defenses are no longer adequate. Leading organizations are adoption "perimeter-less" cybersecurity frameworks, using a Zero Trust architecture.

What is Zero Trust? Is an approach to cybersecurity and risk management that safeguards the environment no matter where data and people reside. It is not a product. It is a framework or model that leading organizations use to build the capability to **trust nothing and verify everything.**

Zero Trust requires stringent security validation within every aspect of the organization. Cybersecurity defenses shift focus from static, network-based perimeters to users, assets, and resources. It grants no implicit trust based solely on physical or network location or ownership.

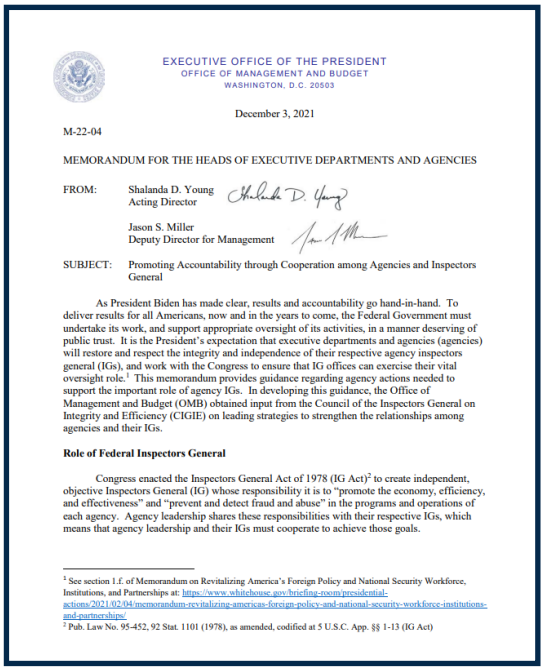
Read full article: Journal of Government Financial Management, Summer 2021



OMB Memo (M-22-04)

Promoting Accountability through Cooperation among Agencies and Inspector Generals

"As President Biden has made clear, results and accountability go hand-in-hand. To deliver results for all Americans, now and in the years to come, the Federal government must take undertake its work, and support appropriate oversight of its activities, in a manner deserving of public trust. It is the President's expectation the executive departments and agencies will restore and respect the integrity and independence of their respective agency inspectors general and work with the Congress to ensure that IG offices can exercise their vital oversight role. This memorandum provides guidance regarding agency actions needed to support the important role of agency IGs. In developing this guidance, the Office of Management and Budget (OMB) obtained input from the Council of Inspectors General on Integrity and Efficiency on leading strategies to strengthen the relationships among agencies and their IGs."



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

December 3, 2021

M-22-04

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

Jason S. Miller
Deputy Director for Management

SUBJECT: Promoting Accountability through Cooperation among Agencies and Inspectors General

As President Biden has made clear, results and accountability go hand-in-hand. To deliver results for all Americans, now and in the years to come, the Federal Government must undertake its work, and support appropriate oversight of its activities, in a manner deserving of public trust. It is the President's expectation that executive departments and agencies (agencies) will restore and respect the integrity and independence of their respective agency inspectors general (IGs), and work with the Congress to ensure that IG offices can exercise their vital oversight role.[1] This memorandum provides guidance regarding agency actions needed to support the important role of agency IGs. In developing this guidance, the Office of Management and Budget (OMB) obtained input from the Council of the Inspectors General on Integrity and Efficiency (CIGIE) on leading strategies to strengthen the relationships among agencies and their IGs.

Role of Federal Inspectors General

Congress enacted the Inspectors General Act of 1978 (IG Act)[2] to create independent, objective Inspectors General (IG) whose responsibility it is to "promote the economy, efficiency, and effectiveness" and "prevent and detect fraud and abuse" in the programs and operations of each agency. Agency leadership shares these responsibilities with their respective IGs, which means that agency leadership and their IGs must cooperate to achieve those goals.

[1] See section 1.f. of Memorandum on Revitalizing America's Foreign Policy and National Security Workforce, Institutions, and Partnerships at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/04/memorandum-revitalizing-americas-foreign-policy-and-national-security-workforce-institutions-and-partnerships/

[2] Pub. Law No. 95-452, 92 Stat. 1101 (1978), as amended, codified at 5 U.S.C. App. §§ 1-13 (IG Act)

Sections:

1. Role of Federal Inspectors General
2. Role of OMB
3. American Rescue Plan Implementation Lessons Learned
4. Agency Actions to Demonstrate and Reinforce Cooperation with IGs

See **Attachment 1** Framing Language from CIGIE for Agency Communications on OIG Cooperation and Access.

Read original memo: [Promoting Accountability through Cooperation among Agencies and Inspectors General (whitehouse.gov)]

Training & Development Opportunities

DECEMBER 2021	Performance Measures 101	Performance Measures 101 (Federal Employees Only) Tickets, Fri, Dec 10, 2021 at 10:00 AM | Eventbrite
	Data Literacy	Data Literacy (Federal Employees Only) Tickets, Fri, Dec 17, 2021 at 10:00 AM | Eventbrite
JANUARY 2022	TECHRISK	https://www.rims.org/events/rf/techrisk-risktech-2022
FEBRUARY 2022	Applying and Integrating ERM	https://www.rims.org/education/online-learning/virtual-workshops/applying-and-integrating-erm
MARCH 2022	Cybersecurity and ERM	https://www.agacgfm.org/Webinars/2021-2022-Webinars/Cybersecurity-ERM.aspx

Be Risk SMART

S	M	A	R	T
Spot	Manage	Act	Realize	Teach
•Spot what can go right or wrong	•Manage what you can	•Act on a decision	•Realize the result	•Teach others what you learned

Upcoming ERMWG Meetings

March 9,2022

June - Stay tuned!

September - Stay tuned!

December - Stay tuned!

Contact oig.erm@oig.dol.gov to be added to ERMWG meeting invitations **or you may contact Jessica Southwell or Temika Edwards directly.**

SAVE THE DATE — Next CIGIE ERM Quarterly Meeting will be on Wednesday, March 9, 2022.

If you have recommendations or ideas for future ERM newsletters, feel free to reach out to: Jessica Rivera at jessica.rivera@usdoj.gov.

Available now on the CIGIE ERM Working Group webpage, under ERM Resources.

ERMWG Chair/Co-Chair

Jessica Southwell, DOL OIG

Temika Edwards, HUD OIG

ERMWG Support

Jessica Rivera, DOJ OIG

Tamarah Fosso, DOL OIG

Submissions to ERM Times

Submit articles or other content to ERM Times at oig.erm@oig.dol.gov.

Contact ERMWG

For further information on the CIGIE ERM Working Group, contact oig.erm@oig.dol.gov or Jessica Southwell southwell.jessica@oig.dol.gov or Temika Edwards at tedwards@hudoig.gov

ERMWG Sub-Groups

Implementing an ERM Risk Assessment Approach for Audit Planning Purposes

Co-Chairs:

Shellie Purnell-Brown , FEC OIG
Jonelle Pianta, HUD OIG

Auditing ERM Implementation at Component Agencies

Chair: Rebecca Sharek, SEC OIG

ERM at Small OIGs

Chair: Nick Novak