

Combating Fraud, Waste, Abuse & Mismanagement · Architect of the Capitol



Evaluation of the Architect of the Capitol's Supply Chain Risk Management

2024-0003-IE-P

September 4, 2025



MISSION

The OIG promotes efficiency and effectiveness to deter and prevent fraud, waste and mismanagement in AOC operations and programs. Through value-added, transparent and independent audits, evaluations and investigations, we strive to positively affect the AOC and benefit the taxpayer while keeping the AOC and Congress fully informed.

VISION

The OIG is a high-performing team, promoting positive change and striving for continuous improvement in AOC management and operations. We foster an environment that inspires AOC workforce trust and confidence in our work.



REPORT FRAUD, WASTE AND ABUSE



Confidential Toll-Free Hotline: 877.489.8583



OIG Website & Hotline Report: <https://aocoig.oversight.gov/>



LinkedIn: <https://www.linkedin.com/company/aocoig>



X: [@aocoig](https://twitter.com/aocoig)



Email: hotline@aoc-oig.org



Visit: Fairchild Building, Suite 518, 499 South Capitol Street, SW, Washington, DC 20515

Results in Brief

Evaluation of the Architect of the Capitol's Supply Chain Risk Management

SEPTEMBER 4, 2025



OBJECTIVE

The objective of this evaluation was to determine the extent to which the Architect of the Capitol (AOC) implemented an organizational Supply Chain Risk Management (SCRM) process and program that identified, assessed, mitigated, and responded to supply chain risks throughout the agency. Additionally, to determine if vulnerabilities exist for fraud, waste, abuse, and mismanagement.

The AOC has not defined SCRM in the context of its organization, therefore, we used the definition provided by the National Institute of Standards and Technology (NIST) to complete our evaluation. The NIST defines SCRM as a systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplies product and its subcomponents, or the supply chain.

This evaluation was consistent with our 2023 Risk Assessment that listed Program/Project Risk as a key risk domain and our 2024 agency Management Challenges that listed Waste and Accountability as a Management Opportunity and Performance Challenge.

FINDINGS

Based on the results of our work, we identified two findings:

- AOC lacks a supply chain risk management governance program,
- AOC offices' and jurisdictions' risk management process lacks consistency.

Our report describes these areas that reduced the effectiveness of AOC's risk program in more detail. These findings represent gaps that may pose risks to the AOC.

RECOMMENDATIONS

We made three recommendations to strengthen AOC's risk program. Specifically, we recommend AOC:

- 1a.)** Perform an independent risk assessment to identify and evaluate potential risks within the agency's supply chain, including risks related to cybersecurity, geopolitical factors, vendor reliability, and compliance with regulatory requirements. This assessment will allow the agency to determine whether a formal SCRM program is necessary based on the agency's unique risk profile, and
- 1b.)** If deemed necessary based on the outcomes of the assessment performed, develop and implement a SCRM program tailored to the identified risks. This may

Results in Brief Continued

include implementing or enhancing appropriate controls, vendor risk management processes, continuous monitoring, and integration of risk considerations into procurement and operation decision-making.

2. Define, document, and implement risk management processes for offices and jurisdictions to consistently identify, track, and manage risks applicable to them.
3. Develop and document risk tolerance thresholds for strategic objectives.

MANAGEMENT COMMENTS

The AOC provided comments on August 20, 2025, see Appendix C. In its management comments, the AOC concurred with two of the OIG's recommendations and partially concurred with one recommendation.

Please see the Recommendations Table on the following page.

RECOMMENDATIONS TABLE

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Architect of the Capitol		1a, 1b, 2 and 3	None

We received the AOC's Management Comments on August 20, 2025.

The following categories are used to describe agency management's comments to individual recommendations:

- **Open Unresolved:** Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **Open Resolved:** Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **Closed:** OIG verified that the agreed upon corrective actions were implemented.



Inspector General

DATE: September 4, 2025

TO: Thomas E. Austin, PE, CCM, PMP
Architect of the Capitol

FROM: Luiz A. Santos, CFE, PMP
Inspector General

SUBJECT: Evaluation of Architect of the Capitol's Supply Chain Risk Management
(2024-0003-IE-P)

The Architect of the Capitol (AOC) Office of Inspector General (OIG) is transmitting Sikich's evaluation of the AOC's Supply Chain Risk Management. Under contract AOCSSB22A0007-F014 monitored by my officer, Sikich, an independent public accounting firm, performed the evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's (CIGIE's) Quality Standards for Inspection and Evaluation (Blue Book), December 2020.

Our report concluded that the AOC lacks a defined supply chain risk management program, and that inconsistencies are prevalent within the AOC's offices and jurisdictions risk management process. Furthermore, we determined that the AOC should enhance supply chain risk management and risk assessment processes and procedures. This report contains two findings and three recommendations on the AOC's supply chain risk management process.

In response to our official draft report (Appendix C), you concurred with two of our recommendations and partially concurred with one recommendation. We feel the proposed corrective actions address our recommendations. However, the status of the recommendations will remain open until final corrective action is taken. We will contact you within 90 days to follow up on the progress of your proposed management decision.

We appreciate the courtesies extended to the staff during the evaluation. Please direct questions to Chico Bennett, Assistant Inspector General for Inspections and Evaluations, at 202.394.2391 or Chico.Bennett@aoc.gov.

Distribution List:

- Joseph Campbell, Deputy Architect
- Patrick Briggs, Chief of Staff
- Danna Planas Ocasio, Deputy Chief of Staff
- Joseph DiPietro, Chief of Operations
- Telora Dean, Chief Administrative Officer
- Sherri Jordan, Chief Financial Officer
- Aaron Altwies, Chief Security Officer
- Harold Honegger, Chief, Acquisition of Supplies, Services and Materials Management Division
- Curtis McNeil, Risk Management Officer
- Angela Freeman, General Counsel

TABLE OF CONTENTS

RESULTS IN BRIEF	I
Objective	i
Findings	i
Recommendations	i
Management Comments	ii
INTRODUCTION	1
Objective	1
Background	1
Criteria	8
Summary of Results	9
DETAILED EVALUATION RESULTS	9
Finding 1: Lack of a Supply Chain Risk Management Governance Program	9
Conclusion	11
Recommendations	11
Finding 2: AOC Offices' and Jurisdictions' Risk Management Process Lacks Consistency	13
Conclusion	14
Recommendations	14
CONSIDERATIONS OF SUPPLY CHAIN RISKS RELEVANT TO THE AGENCY	17
APPENDIX A	19
Scope and Methodology	19
APPENDIX B	21
Notification Letter	21
APPENDIX C	22
Management Comments	22
ACRONYMS AND ABBREVIATIONS	26

INTRODUCTION

Objective

The Architect of the Capitol (AOC) Office of Inspector General (OIG) contracted with Sikich CPA LLC (“Sikich”) to perform an evaluation to determine the extent to which the AOC implemented an organizational Supply Chain Risk Management (SCRM) process and program that identified, assessed, mitigated, and responded to supply chain risks throughout the agency. Additionally, as part of the evaluation, Sikich also determined if vulnerabilities exist for fraud, waste, abuse, and mismanagement, as a result of control deficiencies in the SCRM process.

Sikich evaluated the AOC’s SCRM processes from Fiscal Year (FY) 2019 to FY 2024 for the following offices and jurisdictions:

- Office of the Chief Security Officer (OCSO)
- Information Technology Division (ITD)
- Capitol Power Plant
- House Office Buildings

We conducted this evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency’s (CIGIE)¹ *Quality Standards for Inspection and Evaluation*. Those standards require us to plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives. Appendix A contains more information about our scope and methodology to achieve the objective.

Background

To better understand the scope of this work, we outlined the key components below:

1. Provide contextual background on the agency, including a summary of its offices and jurisdictions encompassed by our evaluation.
2. Define SCRM, detailing the nature of supply chain risks and their strategic importance.
3. Outline the criteria used to guide this evaluation.
4. Provide a summary of results.

¹ CIGIE is an independent entity established within the executive branch to address integrity, economy and effectiveness issues that transcend individual Government agencies and aid in the establishment of a professional well-trained and highly skilled workforce in the Offices of Inspector General. Retrieved from CIGIE website: <https://www.ignet.gov/IGNET | Council of the Inspectors General on Integrity and Efficiency: IGnet>

The scope of this engagement was the implementation of the AOC's SCRM processes and operations from FY 2019 to FY 2024. To meet our objective, we evaluated supply chain risks at the enterprise level and the extent to which the following offices and jurisdictions consider supply chain risk: OCSO, ITD, Capitol Power Plant, and House Office Buildings. In addition to the four offices and jurisdictions, Sikich also conducted inquiries with the Integrated Risk Management Division (IRMD) and Procurement offices to understand its involvement in assessing supply chain risks. Information regarding these offices and jurisdictions is outlined below.

Organizational Background

Established as a permanent office in 1876, the Architect² is provided permanent authority for the care and maintenance of the United States Capitol based on Section 1811 of Title 2 of the United States Code. The Architect is responsible for the maintenance, operation, development and preservation of 18.5 million square feet of buildings and more than 570 acres of land throughout Capitol Hill. The Architect also provides professional expertise with regard to the preservation of architectural and artistic elements entrusted to their care and provides recommendations concerning design, construction and maintenance of the facilities and grounds.

Office of the Chief Security Officer

The OCSO is responsible for the maintenance, care and operation of the buildings, grounds and physical security enhancements of the United States (U.S.) Capitol Police, campus-wide physical security infrastructure and an off-site campus supporting other legislative branch agencies.

The OCSO oversees the execution of security related and sensitive facility and infrastructure projects. The OCSO also coordinates interagency emergency preparedness and manages internal security programs and policies, including personnel suitability and badging, continuity of operations, critical infrastructure and resiliency programs and the emergency management program.

Information Technology Division

The ITD resides within the Office of the Chief Administrative Officer, which provides information technology (IT) leadership, solutions and user support on and off the Capitol campus. The ITD consists of four branches:

² The AOC is both the name of the U.S. legislative branch agency and the title of the leader of the agency (referred to as the Architect). Retrieved from: <https://www.aoc.gov/about-us/organizational-structure>.

- Application Development and Support Branch
- Information Security Branch
- Infrastructure Management Branch
- Customer Engagement Branch

Each of the branch chiefs is a part of the ITD Project Portfolio Management Office, which is responsible for establishing and managing the alignment of ITD resources to AOC business priorities.

Capitol Power Plant

The Capitol Power Plant provides steam and chilled water used to heat and cool buildings throughout the U.S. Capitol campus. In December 1910, the plant started operations, generating steam and electricity for the U.S. Capitol Building. In 1951, it ceased generating electricity. At the same time the plant's electricity generating capacity had reached its limit and it was therefore decided to abandon production and transfer loads to the local electrical utility, Potomac Electric Power Company (PEPCO).³ The plant has been enlarged many times to keep up with expansion of congressional offices and corresponding increase in heating and cooling demands of the U.S. Capitol.

The Capitol Power Plant was authorized in 1904 to support new office buildings which were then in the early planning stages. These new facilities, now known as the Cannon House Office Building and the Russell Senate Office Building, required substantial heating and electrical supplies that were to be generated remotely. In addition, the U.S. Capitol and the Library of Congress would also be tied into the new plant, as would be all future buildings constructed on the Capitol campus.

Construction of the U.S. Capitol Visitor Center prompted the plant's expansion in the early 21st Century. The Capitol Power Plant jurisdiction manages the year-round operation of the power plant, providing steam and chilled water to heat and cool the U.S. Capitol and 22 other facilities on or around Capitol Hill.

In addition to the central steam and refrigeration plants, the jurisdiction also maintains an administration building and the utility tunnel distribution and metering system.

House Office Buildings

The House Office Buildings jurisdiction is responsible for the operation, maintenance and preservation of more than five million square feet of facility space, including the Cannon House Office Building, Ford House Office Building, Longworth House Office Building, O'Neill House Office Building and Rayburn House Office Building, underground garages, annexes and tunnels.

³ PEPCO is a member of the Exelon family of companies and serves as the Mid-Atlantic region's leading electric and gas utility company. PEPCO delivers energy to customers in the District of Columbia (D.C.) and Maryland. Retrieved from PEPCO website: [Company Information | Pepco - An Exelon Company](#)

The jurisdiction provides facility repairs and maintenance for building infrastructure, performs client services, conducts building and safety inspections, responds to emergencies, addresses compliance issues, executes abatement and implements energy savings initiatives. Additionally, the jurisdiction serves as an agent of the House of Representatives, representing the interests of congressional operations during capital projects or building renewals. The AOC employs professionals across multiple areas of expertise, including architecture, electricity, engineering, gardening, historic preservation, masonry, mechanics, painting and plaster, plumbing, sheet metal, visitor services, and wood crafting. Additionally, the AOC is undergoing multiple major projects and preservation efforts, including: Cannon House Office Building Renewal (CHOB) Project, Heritage Asset Conservation, and Stone Preservation on the Capitol Campus.

Integrated Risk Management Division

The IRMD, which operates under the Office of the Chief Financial Officer, oversees the AOC's Enterprise Risk Management (ERM) Program. The IRMD is led by the Risk Management Officer (RMO), and performs the following:

- Facilitates and advances the ERM process
- Provides risk management subject matter expertise to AOC personnel
- Collects and analyzes risk data to enable risk-informed, data-driven decisions
- Elevates risk insights and intelligence to the Executive Risk Committee (ERC)⁴ and Risk and Control Working Group (RCWG)⁵
- Collaborates with the ERC and RCWG to monitor and update AOC's Risk Profile
- Promotes a culture of awareness across all levels of the agency
- Provides ERM-related training, as needed

Procurement

The Acquisition and Material Management Division (AMMD) delivers acquisition and material management support solutions. Sikich noted there are two divisions within AMMD that are significant to AOC's procurement functions: the Supplies, Services and Material Management Division (SSMMD) and the Design & Construction Acquisition Division (DCA).

The SSMMD are business advisors for the procurement of supplies and services, the Personal Property Management and Fleet Management programs and the Purchase Card and Small Business programs at the AOC. The SSMMD team are contract specialists that guide AOC personnel through the procurement process and assist in the development of contracting documents.

The DCA are business advisors for Architect/Engineering, Construction and Construction Management support services. The DCA Contracting Specialists assist AOC personnel with acquisition planning and formulation of contracts to help execute the AOC's mission in a timely

⁴ The ERC was established by the Architect of the Capitol and the RMO to oversee and guide efforts of the ERM Program and advise the Architect of the Capitol on making risk-informed decisions.

⁵ The RCWG provides mission-level governance, accountability, transparency and oversight for the active management of enterprise-level or significant risks identified through the annual risk assessment process and for embedding ERM into core business functions.

fashion. Additionally, DCA is the office of primary responsibility for AOC Order 34-1 Contracting Manual.

The AOC's Contracting Manual provides ongoing and current policy and procedures for the acquisition of supplies, services and construction, and provides guidance to staff applying those policies and procedures. Certain sections have been revised to allow the AOC to incorporate some best practices consistent with the Federal Acquisition Regulation (FAR).⁶

Supply Chain Risk Management

Defining Supply Chain Risk Management

The National Institute of Standards and Technology (NIST) defines SCRM as a systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplies product and its subcomponents, or the supply chain.⁷

Understanding Supply Chain Risk Management

According to the Federal Bureau of Investigation (FBI),⁸ the globalization of the U.S. economy presents unique and complex challenges when applying SCRM methodologies to safeguard the U.S. Government (USG) supply chain from emerging threats and vulnerabilities. The presence and influence of foreign governments, poor manufacturing and/or development practices, counterfeit products, tampering, theft, malicious software, etc. are examples of supply chain risks that must be mitigated. Federal agencies, government contractors, suppliers, and integrators use varied and non-standardized practices, making it difficult to consistently evaluate, measure, and neutralize threats to the USG supply chain.

Additionally, the challenge of SCRM has been exacerbated by globalization, where even sensitive products like defense systems use raw materials, circuit boards, and related components that may have originated in countries where the system manufacturer did not even know it had a supply chain. This increased complexity has brought with it more potential failure points and higher levels of risk.

Organizations are concerned about the risks associated with products and services that may potentially contain malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the supply chain. These risks are associated with an enterprise's decreased visibility into and understanding of how the technology they

⁶ The FAR is the primary regulation for use by all executive agencies in their acquisition of supplies and services with appropriated funds. The FAR contains standard solicitation provisions and contract clauses and the various agency FAR supplements. The FAR is jointly issued by the Department of Defense (DoD), General Services Administration (GSA), and the National Aeronautics and Space Administration. Retrieved from GSA website: <https://www.gsa.gov/policy-regulations/regulations/federal-acquisition-regulation-far>

⁷ Retrieved from: https://csrc.nist.gov/glossary/term/supply_chain_risk_management

⁸ The FBI published *Best Practices in Supply Chain Risk Management for the U.S. Government* (February 2016), which Sikich leveraged as guidance to conduct our evaluation.

acquire is developed, integrated, and deployed or the processes, procedures, standards, and practices used to ensure the security, resilience, reliability, safety, integrity, and quality of the products and services.

In 2018, the U.S. government stood up multiple agencies and task forces to better address supply-chain risk (including the Critical Infrastructure Security and Cybersecurity Agency in the Department of Homeland Security and the Protecting Critical Technology Task Force at the Department of Defense (DoD)), and the private sector continues to seek a uniform and proven methodology for assessing and monitoring risks in a way that truly minimizes business disruption.

The DoD noted they require healthy, resilient, diverse, and secure supply chains to ensure the development and sustainment of capabilities critical to national security. The coronavirus disease (COVID-19) pandemic highlighted vulnerabilities in complex global supply chains in very real ways to the public, government, and industry. Beyond COVID-19, supply chain disruptions have become more frequent and severe overall. Additionally, the DoD noted national resolve to strengthen America's supply chains is not limited to the Executive Branch. Congress has demonstrated a commitment to renewing and strengthening U.S. manufacturing through the Bipartisan Infrastructure Law and the House Armed Services Committee critical supply chain task force. The Defense Industrial Base and related trade associations have outlined myriad actions and are actively engaging with the government at all levels to build resiliency. The DoD is committed to strengthening the industrial base and establishing a network of domestic and allied supply chains to meet national security needs.

Overall, supply chain risks are emerging as a critical area of concern that agencies must proactively assess. The following subsections provide an overview of SCRM and highlight the key components of an effective SCRM program as integrated into existing risk management activities.

Key Elements of an Effective Supply Chain Risk Management Program

According to the FBI, federal agencies should develop a SCRM strategy that accounts for known and emerging threats, vulnerabilities, and organizational impacts. Federal agency supply chains are as unique as the individual agencies they support. A good SCRM program will require USG agencies to establish a coordinated team approach to assess supply chain risks and actions necessary to mitigate the risk to an acceptable level. The backbone of the team should consist of a diverse group of professional disciplines with expertise in SCRM, security, procurement, contract and administrative law, audit and finance, and facilities management. An agency's SCRM program should leverage a variety of resources, including open-source commercial products, to build a risk assessment baseline that includes a potential vendor's legal history, financial solvency, tax history, and corporate relations. The agency's initial research should be combined with a detailed risk assessment focused on counterintelligence threats.

According to McKinsey & Company,⁹ organizations should invest time with a cross-functional team to catalog the full scope of risks they face, including identifying gray areas where risks are hard to understand or define (e.g., tiers of the supply chain where no visibility exists). This analysis can illustrate the scale and scope of unknown risks. Unknown risks are those that are impossible or very difficult to foresee. For unknown risks, reducing their probability and increasing the speed of response when they do occur is critical to sustaining competitive advantage. Managing unknown risks is best achieved through creating strong defenses combined with building a risk-aware culture. Strong defenses, from request-for-proposal (RFP) language to worker training, all contribute to an organization identifying and stopping unknown risks before they affect operations. To manage known risks, organizations can use a combination of structured problem solving and digital tools to effectively manage their known-risk portfolio through four steps:

1. Identify and document risks

- A typical approach for risk identification is to map out and assess the value chains of all major products. Each node of the supply chain — suppliers, plants, warehouses, and transport routes — is then assessed in detail. Risks are entered into a risk register and tracked on an ongoing basis. In this step, parts of the supply chain where no data exist and further investigation is required should be recorded.

2. Build a SCRM framework

- Every risk in the register should be scored based on three dimensions to build an integrated risk-management framework: impact on the organization if the risk materializes, the likelihood of the risk materializing, and the organization's preparedness to deal with that specific risk. Tolerance thresholds are applied on the risk scores reflecting the organization's risk appetite.

3. Monitor Risk

- Once a risk-management framework is established, persistent monitoring is one of the critical success factors in identifying risks that may damage an organization. The recent emergence of digital tools has made this possible for even the most complex supply chains, by identifying and tracking the leading indicators of risk. Successful monitoring systems are customized to an organization's needs, incorporating impact, likelihood, and preparedness perspectives. It is critical to have an early warning system to track top risks to maximize the chances of mitigating, or at the very least limiting, the impact from their occurrence.

4. Institute governance and regular review

- The final critical step is to set up a robust governance mechanism to periodically review supply chain risks and define mitigating actions, improving the resilience and agility of the supply chain. An effective SCRM governance mechanism is a cross-functional risk

⁹ McKinsey & Company published [*A Practical Approach to Supply-Chain Risk Management*](#) (March 2019), which Sikich leveraged as guidance to conduct our evaluation.

board with participants representing every node of the value chain. It typically includes line managers who double-hat as risk owners for their function, giving them ownership of risk identification and mitigation. An effective risk board will meet periodically to review the top risks in the supply chain and define the mitigation actions. The participants will then own the execution of mitigation actions for their respective functional nodes. Additionally, in many organizations the risk board will also make recommendations to improve the agility and resilience of the supply chain, ranging from reconfiguring the supply network, finding new ways of reducing lead times, or working with suppliers to help optimize their own operations. Increasing supply-chain agility can be a highly effective mitigation strategy for organizations to improve their preparedness for a wide range of risks.

Criteria

The AOC has not formalized a definition for SCRM. As such, Sikich utilized the definition provided by the NIST to perform its evaluation. According to NIST:

“SCRM is the process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplies product and its subcomponents, or the supply chain.”

Table 1 outlines other standards and guidance used to guide our evaluation.

Table 1: Standards and Guidance

Standard / Guidance	Publication Date
Best Practices in Supply Chain Risk Management for the U.S. Government, FBI	February 2016
Securing Defense-Critical Supply Chains: An Action Plan Developed in Response to President Biden's Executive Order 14017, DoD	February 2022
Vendor Supply Chain Risk Management Template, Cybersecurity and Infrastructure Security Agency, National Management Center	April 2021
A Practical Approach to Supply-Chain Risk Management, McKinsey & Company	March 2019
Standards for Internal Control in the Federal Government (referred to as "The Green Book"), Government Accountability Office	September 2014
Office of Management and Budget (OMB) Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control	July 2016
NIST Special Publication 800-161, Update 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations	May 2022

Summary of Results

Based on the results of our work, we identified the agency's lack of a SCRM governance program and AOC's offices' and jurisdictions' risk management process lacks consistency. The next section discusses these evaluation results in more detail.

DETAILED EVALUATION RESULTS

The following section of the report describes the evaluation results in more detail.

Finding 1: Lack of a Supply Chain Risk Management Governance Program

According to the FBI, federal agencies should develop a SCRM strategy that accounts for known and emerging threats, vulnerabilities, and organizational impacts. Federal agency supply

chains are as unique as the individual agencies they support. No one SCRM strategy can be universally applied across the federal government, but federal agencies should follow the established NIST SCRM standards as a foundation of their own strategy. SCRM standards will require USG agencies to establish a coordinated team approach to assess supply chain risk and actions necessary to mitigate the risk to an acceptable level.

The backbone of the team should consist of a diverse group of professional disciplines with expertise in SCRM, security, procurement, contract and administrative law, audit and finance, and facilities management. SCRM should leverage a variety of resources, including open-source commercial products, to build a risk assessment baseline that includes a potential vendor's legal history, financial solvency, tax history, and corporate relationships. Initial research should be combined with a detailed risk assessment focused on counterintelligence threats.

However, the agency has not consistently considered or defined supply chain risks at the enterprise or jurisdiction/office levels and lacks policies and procedures to do so. As such, the agency has not established or performed the following:

- Not all jurisdictions and offices have established points of contact (POCs) responsible for identifying, communicating, and responding to supply chain risks in tandem with the IRMD.
- The agency has selectively not incorporated all SCRM related FAR clauses into its contracts, such as, clauses 52.204-23, 52.204-24, 52.204-25, 52.204-26, 52.204-28, 52.204-29, and 52.204-30.¹⁰
- Offices and jurisdictions have not consistently identified key supplies and suppliers relevant to their operations. Additionally, supplier risk profiling and critical suppliers' financial stability and production capacity are not consistently assessed.
- Offices and jurisdictions have not consistently developed buffer stock or inventory management strategies. For example:
- Inventory systems lack real-time tracking, which could lead to delays during emergencies or budget freezes.
- None of the evaluated offices or jurisdictions conduct regular scenario planning or stress testing to identify responses to supply chain disruptions.

As such, the AOC has not instituted a SCRM program due to the following considerations:

- As a Legislative Branch Agency, the AOC is not subject to the mandatory requirements of NIST or FAR standards and regulations, and
- No immediate or significant risks to the AOC's supply chain have been self-identified by the agency that warrant the development and implementation of such a program.

¹⁰ The following FAR clauses are titled: 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities, 52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment, 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment, 52.204-26 Covered Telecommunications Equipment or Services-Representation, 52.204-28 Federal Acquisition Supply Chain Security Act Orders – Federal Supply Schedules, Governmentwide Acquisition Contracts, and Multi-Agency Contracts, 52.204-29 Federal Acquisition Supply Chain Security Act Orders – Representation and Disclosures, and 52.204-30 Federal Acquisition Supply Chain Security Act Orders – Prohibition. Retrieved from: <https://www.acquisition.gov/sites/default/files/current/far/pdf/FAR.pdf>

Without an agency-wide definition of SCRM and overarching policy and guidance regarding supply chain risks, the AOC and its offices and jurisdictions could face the following potential operational disruptions across the AOC campus:

- **Disruptions in Mission-Critical Services:** without clearly identified critical supplies, contingency plans, and contract clauses, the agency is more vulnerable to disruptions that can delay or halt essential operations, especially during emergencies or high-demand periods. Additionally, without a structured program, the agency may be unaware of or unprepared for threats such as disruptions from geopolitical conflicts or natural disasters and vendor insolvency or performance failures.
- **Inefficient Emergency Response:** the absence of buffer stock strategies and scenario planning can leave the agency unprepared to respond to sudden supply shocks, such as pandemics, natural disasters, or geopolitical events.
- **Increased Downtime and Delays:** without real-time inventory tracking, offices may run out of key supplies or overstock unneeded items, leading to inefficiencies, delays, and resource waste.
- **Financial Impacts:** without a proactive SCRM strategy, the agency may rely on emergency purchasing, which typically comes at a premium, especially when demand is high or supply is constrained.
- **Reputational Damage:** security vulnerabilities or unethical sourcing practices could erode public trust in the AOC's ability to protect critical government infrastructure and uphold ethical standards.
- **No Clear Accountability:** without a designated POC or responsible party for supply chain risks, issues may go unnoticed or unaddressed until they escalate into full-blown crises.
- **Inability to Adapt to Evolving Threats:** failure to perform scenario planning and stress testing limits the agency's ability to identify emerging risks or adapt to changing environments (i.e., cybersecurity threats, supplier insolvency, or geopolitical instability).

Conclusion

The agency's lack of a defined and implemented comprehensive SCRM strategy poses potentially serious operational and strategic risks. The agency lacks designated POCs, consistent identification of key suppliers, and important policies, procedures, and processes such as the incorporation of FAR related SCRM clauses, buffer stock planning, scenario planning, and stress testing. These deficiencies pose the potential to undermine the agency's ability to respond efficiently to disruptions, increasing the risk of service delays, financial losses, reputational harm, and operational downtime.

Recommendations

Recommendation 1a

We recommend the Architect of the Capitol perform an independent risk assessment to identify and evaluate potential risks within the agency's supply chain, including risks related to

cybersecurity, geopolitical factors, vendor reliability, and compliance with regulatory requirements. This assessment will allow the agency to determine whether a formal Supply Chain Risk Management program is necessary based on the agency's unique risk profile.

Recommendation 1a – AOC Comment

The AOC concurs. AOC's Office of the Chief Financial Officer, IRMD, will conduct an independent risk assessment as part of the ERM Program's annual risk assessment process to effectively evaluate potential risks within the agency's supply chain. The Office of the Chief Financial Officer, IRMD, will share the results of the risk assessment with the ERM Governance bodies, the Executive Risk Committee and the Risk and Control Working Group, to determine the most effective way forward.

Recommendation 1a – OIG Comment

The OIG recognizes the AOC's concurrence with the recommendation. The AOC's actions appear to be responsive to the recommendation. Therefore, the recommendation is considered resolved but open. The recommendation will be closed upon completion and verification of the proposed actions.

Anticipated Completion: May 2026

Recommendation 1b

If deemed necessary based on the outcomes of the assessment performed, develop and implement a Supply Chain Risk Management program tailored to the identified risks. This may include implementing or enhancing appropriate controls, vendor risk management processes, continuous monitoring, and integration of risk considerations into procurement and operation decision-making.

Recommendation 1b – AOC Comment

AOC concurs with the recommendation. If deemed necessary based on the outcomes of the assessment, AOC's Office of the Chief Financial Officer, IRMD, in collaboration with the ERM Governance bodies, the Executive Risk Committee and the Risk and Control Working Group, will determine the most effective and value-added approach to implement supply chain risk management within the agency.

Anticipated Completion: September 2026

Recommendation 1b – OIG Comment

The OIG recognizes the AOC's concurrence with the recommendation. The AOC's actions appear to be responsive to the recommendation. Therefore, the recommendation is considered

resolved but open. The recommendation will be closed upon completion and verification of the proposed actions.

Finding 2: AOC Offices' and Jurisdictions' Risk Management Process Lacks Consistency

The OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, defines Risk Tolerance as “the acceptable level of variance in performance relative to the achievement of objectives. It is generally established at the program, objective or component level. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite.” OMB A-123 notes that the development of an Agency risk profile captures the reasons for decisions made about risk tolerances. Additionally, OMB A-123 states Chief Risk Officers or equivalent function generally work with business unit managers within their organizations to identify issues in a timely manner to allow for proactive management of the program and facilitate informed, data-driven decision-making. The Green Book states management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives. As part of establishing an organizational structure, management establish reporting lines defined at all levels of the organization so units can communicate the quality information necessary for each unit to fulfil its overall responsibilities. Additionally, the Green Book states management should define objectives clearly to enable the identification of risks and define risk tolerances, define risk tolerances in specific and measurable terms so they are clearly stated and can be measured, and evaluate whether risk tolerances enable the appropriate design of internal control by considering whether they are consistent with requirements and expectations for the defined objectives.

However, the agency has not consistently established and implemented the following risk management practices:

- Jurisdiction-level risks and program-level risks are not identified, tracked, and managed consistently across offices and jurisdictions.
- Every jurisdiction within the AOC is responsible for managing its own individual risks; however, there are no designated POCs in charge of risk management at the jurisdictions.
- The agency has not defined a formal risk tolerance.

The RMO and IRMD are responsible for executing an ERM Program and not a Risk Management Program. As such, there are no required policies and procedures and governing body responsible for managing risks across the jurisdictions and offices that do not escalate to the enterprise level. Additionally, the AOC has elected not to adopt a risk tolerance as suggested by OMB Circular A-123 Guidance.

Without implementing consistent risk management processes across the offices and jurisdictions the agency may fail to identify and mitigate threats and vulnerabilities, such as those associated with SCRM. Without designated POCs, there is no clear responsibility for risk identification, monitoring, and mitigation. In the absence of clear roles, response times in decision making are often slower. Further, offices and jurisdictions managing risks inconsistently may result in duplication of efforts, gaps in coverage, or conflicting actions. Also, undefined POCs can hinder communication across offices and jurisdictions which is critical for understanding interdependencies and cumulative risk exposures.

Additionally, without formally defining and establishing risk tolerance levels, the agency may not ensure strategic alignment, appropriate variation levels for performance measures, facilitate informed decision-making, and promote efficient resource allocation at the enterprise, jurisdiction, and program levels.

Conclusion

The agency's lack of consistent risk management practices, including the absence of designated POCs, undefined risk tolerance levels, and inconsistent identification and tracking of risks across jurisdictions, may create operational vulnerabilities. These gaps may hinder the agency's ability to proactively manage threats, such as those related to supply chain disruptions, and may result in unclear accountability and inefficient resource allocation.

Recommendations

Recommendation 2

We recommend that the agency work with the offices and jurisdictions to define, document, and implement risk management processes for offices and jurisdictions to consistently identify, track, and manage risks applicable to them.

Recommendation 2 – AOC Comment

The AOC partially concurs. AOC's Office of the Chief Financial Officer, IRMD already has an Integrated Risk Management Framework (IRMF) Procedural Guide that clearly defines and documents the agency's risk management processes. This Procedural Guide is posted to the AOC's Office of the Chief Financial Officer, IRMD Compass Page within the Resources section and is accessible to everyone in the agency. Specifically, the IRMF Overview section states the following:

"The IRMD's framework is a continuous, systematic process for responding to risks as they emerge. It provides a means to embed structured, disciplined and consistent risk management practices and procedures at the enterprise, jurisdictional and program levels to allow for more informed decision-making and to improve performance at all levels of the agency."

AOC's Office of the Chief Financial Officer, IRMD, will update this documentation and strengthen our communications and socialization efforts to help confirm its contents and purpose are clearly understood and applied throughout the organization. Additionally, we will work with the offices and jurisdictions on implementing these risk management practices to consistently identify, track, and manage risks applicable to them.

Anticipated Completion: September 2026

Recommendation 2 – OIG Comment

The OIG recognizes the AOC's partial concurrence with the recommendation. The AOC's actions appear to be responsive to the recommendation. Therefore, the recommendation is considered resolved but open. The recommendation will be closed upon completion and verification of the proposed actions.

Recommendation 3

We recommend that the agency work with the offices and jurisdictions to develop and document risk tolerance thresholds for strategic objectives.

Recommendation 3 – AOC Comment

The AOC concurs with the recommendation. The conclusion of FY 2025 marks the end of the current AOC Strategic Plan, which covered FY 2022-FY 2025. On October 1, 2025, the AOC will issue an Agency Performance Plan that will include the AOC strategic goals and objectives for the next 3 to 5 years as well as include longer term (next 15 to 20 years) goals to incorporate the Capitol Complex Master Plan (CCMP). Key risk tolerance thresholds will be aligned to the strategic goals and objectives identified in the Agency Performance Plan (if applicable). Once a strategic document is disseminated for agency-wide consumption, AOC's Office of the Chief Financial Officer, IRMD along with the Program Analysis and Evaluation Division, in collaboration with the ERM Governance bodies, the Executive Risk Committee and the Risk and Control Working Group, will determine if establishing risk tolerance thresholds at the Office and Jurisdiction levels is a value-added practice for our agency.

OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, which is guidance referenced within the report Table 1: Standards and Guidance (page 9) makes the following references related to risk appetite and tolerances within an ERM Program:

From OMB A-123, Section A. Governance, page 13:

“Regardless of the governance structure developed, agency governance should include a process for considering risk appetite and tolerance levels. The concept of “risk appetite” is key to achieving effective ERM, and is essential to consider in determining risk responses. Although a formally documented risk appetite statement is not required,

agencies must have a solid understanding of their risk appetite and tolerance levels in order to create a comprehensive enterprise-level risk profile.”

From OMB A-123, C. Implementation, Figure 3, ERM Development and Implementation Deadlines, page 20:

“Agencies are encouraged (not required) to develop an approach to implement Enterprise Risk Management (ERM) which may include:

- planned risk management governance structure,
- process for considering risk appetite and risk tolerance levels,
- methodology for developing a risk profile,
- general implementation timeline, and plan for maturing the comprehensiveness and quality of the risk profiles over time

AOC has deliberately omitted concepts on risk appetite and risk tolerance from its ERM implementation because, under federal guidance (e.g., OMB Circular A-123), establishing a formal risk appetite is recommended, not required. Management assessed our internal operating environment and determined that other foundational elements of ERM would provide greater value at this stage in the program’s maturity. The guidance is intentionally principles-based rather than prescriptive, giving agencies ample latitude to tailor their ERM implementation approaches accordingly. We have exercised the discretion to focus on measures and practices we believe will yield the most effective and sustainable ERM program based on our operating environment, risk culture, and program maturity.

Anticipated Completion: To be determined based on the direction from the agency on its new strategic documentation.

Recommendation 3 – OIG Comment

The OIG recognizes the AOC’s concurrence with the recommendation. The AOC’s actions appear to be responsive to the recommendation. Therefore, the recommendation is considered resolved but open. The recommendation will be closed upon completion and verification of the proposed actions.

Sikich CPA LLC

September 4, 2025

CONSIDERATIONS OF SUPPLY CHAIN RISKS RELEVANT TO THE AGENCY

Though Sikich did not identify any recorded cases of supply chain disruptions or risks that directly impacted agency operations through its evaluation, Sikich did identify areas of the organization that may be more vulnerable to supply chain risks, as detailed below.

- 1. Low Construction RFP Response Rates:** The AOC has many ongoing projects each year to aid in its mission of preserving historic buildings across its campuses, with the most notable being the “CHOBBr project”, which provides an effective workplace for the next century to serve the needs of the U.S. House of Representatives and support Congressional operations. On average, the AOC receives 2.8 proposal responses per RFP for its multiple award construction contracts related RFPs, and 2.3 proposal responses per RFP for its Full and Open RFPs. Low response rates to RFPs for construction contracts may signal underlying supply chain risks that can adversely impact the agency’s ability to execute critical infrastructure projects. A limited pool of bidders can result from restrictive evaluation criteria, labor shortages, off-hour work requirements, or increased project complexity that discourages vendor participation. This lack of competition may lead to higher costs, reduced bargaining power, and increased vulnerability to delays or performance issues. Additionally, a narrower supplier base heightens dependency on a small number of contractors, thereby exposing the agency to heightened risk if one or more vendors experience operational disruptions. Understanding and addressing the factors contributing to low RFP response rates is essential for strengthening procurement resilience and ensuring continuity in project delivery.
- 2. Shortage of Skilled Artisans in the U.S.:** To carry out its operations, AOC employs many individuals skilled in historic preservation, masonry, and painting. For instance, AOC has an ongoing project, “Stone Preservation on the Capitol Campus” to restore the stonework on buildings throughout the Capitol campus. Through our evaluation we noted a shortage of U.S. masonry experts, whereby the agency has had to contract with Italian masonry experts to complete its projects. A shortage of skilled masonry experts capable of preserving the stonework on Capitol buildings to a specific historical time period presents a notable supply chain risk for the agency. This type of restoration work often requires specialized techniques, materials, and knowledge of period-appropriate finishes, significantly narrowing the pool of qualified contractors. Limited availability can lead to project delays, increased costs, and reduced flexibility in scheduling. Moreover, dependence on a small number of niche vendors heightens the risk of disruption should those vendors face capacity issues, labor constraints, or competing project demands. This challenge underscores the importance of proactive workforce planning, early contractor engagement, and strategic sourcing to ensure the agency can meet preservation standards without compromising project timelines or quality.
- 3. Impact of Evolving Foreign Policy on Sourcing Key Supplies:** To carry out its operations to preserve the Capitol buildings, the agency relies on sourced materials such as stone,

metal, and specialized facade components. These materials may be sourced from foreign vendors due to their unique specifications, quality standards, or historical authenticity requirements. However, this dependence exposes the agency to geopolitical and economic factors beyond its control, including fluctuations in global supply chains, shipping delays, and notably, tariffs. Increases in tariffs on imported construction materials can substantially raise project costs, strain budgets, and complicate procurement planning. Moreover, sudden changes in trade policy can disrupt timelines or necessitate last-minute substitutions. To mitigate these risks, the agency must closely monitor trade developments and consider diversifying or sourcing strategies or establishing contingency plans for critical materials.

APPENDIX A

Scope and Methodology

The scope of this evaluation was the AOC's Supply Chain Risk Management Process and Program for the period FY 2019-FY 2024. We conducted this evaluation in Washington, D.C., from September 2024 through May 2025, in accordance with the Council of the Inspectors General on Integrity and Efficiency *Quality Standards for Inspection and Evaluation*. Those standards require us to plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

The AOC OIG self-initiated this evaluation. The objectives of this evaluation were to determine the extent to which the AOC implemented an organizational SCRM process and program that identified, assessed, mitigated, and responded to supply chain risks throughout the agency. Additionally, to determine if vulnerabilities exist for fraud, waste, abuse, and mismanagement.

The scope included assessing the extent to which a SCRM program has been implemented at the enterprise level and for the selection of four offices and jurisdictions. These offices and jurisdictions are outlined in the "Organizational Background" section of the report.

To accomplish our objective, we completed the following procedures:

- Obtained an understanding of previous audits and evaluations relating to the agency's supply chain.
- Inquired with personnel from OCSO, ITD, Capitol Power Plant, and House Office Buildings to gain insights into their supply chain risk considerations and to identify processes used to monitor key suppliers and vendors.
- Inquired of the Procurement divisions to understand contractual clauses it employs to address supply chain risks and their role in acquiring key suppliers and vendors.
- Inquired of IRMD to understand the extent to which supply chain risks are integrated into the agency's Enterprise Risk Management framework.
- Inspected vendor listings to identify the agency's critical suppliers.
- Inspected policies, procedures, and supporting documentation to develop an understanding of the agency's approaches to risk management, procurement, and supply chain considerations.

We utilized the standards and guidance listed in the "Criteria" section of this report to guide our assessment.

We evaluated the extent to which AOC implemented a SCRM process and program. Our work did not include assessing the sufficiency of internal controls over the AOC's SCRM program or other matters not specifically outlined in this report.

Use of Computer-Processed Data

We did not use a material amount of computer-processed data to perform this evaluation.

Prior Coverage

There was no prior coverage of the AOC's supply chain risk management in the preceding five years.

APPENDIX B

Notification Letter




Office of Inspector General
Fairchild Bldg.
499 S. Capitol St., SW, Suite 518
Washington, D.C. 20515
202.593.1948
www.aoc.gov

United States Government
MEMORANDUM

DATE: September 12, 2024

TO: Thomas E. Austin, PE, CCM, PMP
Architect of the Capitol

FROM: Christopher P. Failla, CIG, CFE 
Inspector General

SUBJECT: Announcement for Evaluation of Architect of the Capitol's (AOC's) Supply Chain Risk Management (2024-0003-IE-P)

This is to notify you that the Office of Inspector General (OIG) is initiating an Evaluation of the AOC's Supply Chain Risk Management. Our objective for this evaluation is to determine the extent to which the AOC implemented an organizational supply chain risk management process and program that identifies, assesses, mitigates and responds to supply chain risk throughout the agency. We will also determine if vulnerabilities exist for fraud, waste, abuse and mismanagement. We plan to use external subject matter experts to support us in this effort.

We will contact the appropriate AOC offices to schedule an entrance conference in the upcoming weeks. If you have any questions, please contact Audrey Cree at Audrey.Cree@aoc.gov or 202.231.2682 or Chico Bennett at Chico.Bennett@aoc.gov or 202.394.2391.

Distribution List:

Hajira Shariff, Acting Executive Officer
Patrick Briggs, Chief of Staff
Joseph Di Pietro, Chief of Operations
Telora Dean, Chief Administrative Officer
Harold Honegger, Chief, Supplies, Services and Materials Management Division
Angela Freeman, General Counsel

APPENDIX C

Management Comments



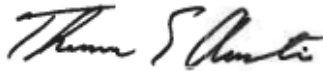
Architect of the Capitol
U.S. Capitol, Room SB-16
Washington, DC 20515
202.228.1793
www.aoc.gov

United States Government

MEMORANDUM

DATE: August 20, 2025

TO: Luiz A. Santos, CFE, PMP
Inspector General

FROM: Thomas E. Austin, PE, CCM, PMP 
Architect of the Capitol

SUBJECT: OIG's Evaluation of the Architect of the Capitol's Supply Chain Risk Management (SCRM) (2024-0003-IE-P)

Thank you for the opportunity to review and comment on the Office of the Inspector General's (OIG) Evaluation of the Architect of the Capitol's (AOC) Supply Chain Risk Management. AOC agrees that conducting an independent risk assessment to identify and evaluate potential risks within the agency's supply chain would be helpful in determining the best way forward. AOC's responses to the OIG's four recommendations can be found below:

Recommendation 1a

We recommend the AOC perform an independent risk assessment to identify and evaluate potential risks within the agency's supply chain, including risks related to cybersecurity, geopolitical factors, vendor reliability, and compliance with regulatory requirements. This assessment will allow the agency to determine whether a formal SCRM program is necessary based on the agency's unique risk profile, and

AOC Response

We concur. AOC's Office of the Chief Financial Officer, Integrated Risk Management Division, will conduct an independent risk assessment as part of the Enterprise Risk Management (ERM) Program's annual risk assessment process to effectively evaluate potential risks within the agency's supply chain. The Office of the Chief Financial Officer, Integrated Risk Management Division, will share the results of the risk assessment with the ERM Governance bodies, the Executive Risk Committee and the Risk and Control Working Group, to determine the most effective way forward.

Anticipated Completion: May 2026

Recommendation 1b

If deemed necessary based on the outcomes of the assessment performed, develop and implement a SCRM program tailored to the identified risks. This may include implementing or enhancing appropriate controls, vendor risk management processes, continuous monitoring, and integration of risk considerations into procurement and operation decision-making.

AOC Response

We concur. If deemed necessary based on the outcomes of the assessment, AOC's Office of the Chief Financial Officer, Integrated Risk Management Division, in collaboration with the ERM Governance bodies, the Executive Risk Committee and the Risk and Control Working Group, will determine the most effective and value-added approach to implement supply chain risk management within the agency.

Anticipated Completion: September 2026

Recommendation 2

We recommend that the agency work with the Offices and Jurisdictions to define, document, and implement risk management processes for Offices and Jurisdictions to consistently identify, track, and manage risks applicable to them.

AOC Response

We partially concur. AOC's Office of the Chief Financial Officer, Integrated Risk Management Division, already has an Integrated Risk Management Framework (IRMF) Procedural Guide that clearly defines and documents the agency's risk management processes. This Procedural Guide is posted to the Office of the Chief Financial Officer, Integrated Risk Management Division's Compass Page within the Resources section and is accessible to everyone in the agency. Specifically, the IRMF Overview section states the following:

"The IRMD's framework is a continuous, systematic process for responding to risks as they emerge. It provides a means to embed structured, disciplined and consistent risk management practices and procedures at the enterprise, jurisdictional and program levels to allow for more informed decision-making and to improve performance at all levels of the agency."

AOC's Office of the Chief Financial Officer, Integrated Risk Management Division, will update this documentation and strengthen our communications and socialization efforts to help confirm its contents and purpose are clearly understood and applied throughout the organization. Additionally, we will work with the offices and jurisdictions on implementing these risk management practices to consistently identify, track, and manage risks applicable to them.

Anticipated Completion: September 2026

Recommendation 3

We recommend that the agency work with the Offices and Jurisdictions to develop and document risk tolerance thresholds for strategic objectives.

AOC Response

We concur. The conclusion of fiscal year (FY) 2025 marks the end of the current AOC Strategic Plan, which covered FY 2022 – FY 2025. On October 1, 2025, the AOC will issue an Agency Performance Plan that will include the AOC strategic goals and objectives for the next 3 to 5 years as well as include longer term (next 15-20 years) goals to incorporate the Capitol Complex Master Plan (CCMP). Key risk tolerance thresholds will be aligned to the strategic goals and objectives identified in the Agency Performance Plan (if applicable). Once a strategic document is disseminated for agency-wide consumption, AOC's Office of the Chief Financial Officer, Integrated Risk Management Division along with the Program Analysis and Evaluation Division, in collaboration with the ERM Governance bodies, the Executive Risk Committee and the Risk and Control Working Group, will determine if establishing risk tolerance thresholds at the Office and Jurisdiction levels is a value-added practice for our agency.

Office of Management and Budget (OMB) Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control, which is guidance referenced within the report Table 1: Standards and Guidance (page 9), makes the following references related to risk appetite and tolerances within an ERM Program:

From OMB A-123, Section A. Governance, page 13:

- “Regardless of the governance structure developed, agency governance should include a process for considering risk appetite and tolerance levels. The concept of “risk appetite” is key to achieving effective ERM and is essential to consider in determining risk responses. **Although a formally documented risk appetite statement is not required,** agencies must have a solid understanding of their risk appetite and tolerance levels in order to create a comprehensive enterprise-level risk profile.”

From OMB A-123, C. Implementation, Figure 3, ERM Development and Implementation Deadlines, page 20:

- “Agencies are encouraged (**not required**) to develop an approach to implement Enterprise Risk Management (ERM) which **may** include:
 - Planned risk management governance structure
 - **Process for considering** risk appetite and risk tolerance levels
 - Methodology for developing a risk profile
 - General implementation timeline
 - Plan for maturing the comprehensiveness and quality of the risk profiles over time”

AOC has deliberately omitted concepts on risk appetite and risk tolerance from its ERM implementation because, under federal guidance (e.g., OMB Circular A-123), establishing a

formal risk appetite is recommended, not required. Management assessed our internal operating environment and determined that other foundational elements of ERM would provide greater value at this stage in the program's maturity. The guidance is intentionally principles-based based rather than prescriptive, giving agencies ample latitude to tailor their ERM implementation approaches accordingly. We have exercised that discretion to focus on measures and practices we believe will yield the most effective and sustainable ERM program based on our operating environment, risk culture, and program maturity.

Anticipated Completion: TBD based on the direction from the agency on its new strategic documentation.

Doc. No. 250813-04-01

ACRONYMS AND ABBREVIATIONS

AMMD	Acquisition and Material Management Division
AOC	Architect of the Capitol
CCMP	Capitol Complex Master Plan
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CHOB	Cannon House Office Building Renewal Project
COVID-19	Coronavirus disease
D.C.	District of Columbia
DCA	Design & Construction Acquisition Division
DoD	Department of Defense
ERC	Executive Risk Committee
ERM	Enterprise Risk Management
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
Green Book	Standards for Internal Control in the Federal Government
GSA	General Services Administration
IRMD	Integrated Risk Management Division
IRMF	Integrated Risk Management Framework
IT	Information Technology
ITD	Information Technology Division
NIST	National Institute of Standards and Technology
OCSO	Office of the Chief Security Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PEPCO	Potomac Electric Power Company
POCs	Points of contact
RCWG	Risk and Control Working Group
RMO	Risk Management Officer
RFP	Request for Proposal
SCRM	Supply Chain Risk Management
SSMMD	Supplies, Services and Material Management Division
U.S.	United States
USG	U.S. Government