



**Architect of the Capitol**

**Office of Inspector General**

**STATEMENT OF  
Management Opportunities  
AND  
Performance Challenges  
FISCAL YEAR 2025**



## MISSION

The Office of Inspector General (OIG) promotes efficiency, effectiveness, and economy to deter and prevent fraud, waste, abuse, and mismanagement in Architect of the Capitol (AOC) programs and operations. OIG does this through value-added, transparent, impactful, and independent audits, inspections, evaluations, and investigations. OIG strives to positively affect the AOC and benefit the taxpayer while keeping the AOC and Congress fully informed.

## VISION

OIG is a high-performing team, promoting positive change and striving for continuous improvement in AOC programs and operations. OIG fosters an environment that inspires AOC workforce trust and confidence in its work.



## REPORT FRAUD, WASTE, AND ABUSE



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



**Email:** [hotline@aac-oig.org](mailto:hotline@aac-oig.org)



**Confidential Toll-Free Hotline:** 877.489.8583



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



**Visit:** Fairchild Building, Suite 518, 499 South Capitol Street, SW, Washington, D.C. 20515

# TABLE OF CONTENTS

---

<b>TRANSMITTAL OF THE FISCAL YEAR 2025 STATEMENT OF MANAGEMENT OPPORTUNITIES AND PERFORMANCE CHALLENGES.....</b>		<b>III</b>
<b>1. SAFETY, SECURITY, AND PRESERVATION MANAGEMENT.....</b>		<b>1</b>
<b>2. INFORMATION AND CYBERSECURITY RISK MANAGEMENT.....</b>		<b>4</b>
<b>3. WORKFORCE MANAGEMENT AND ACCOUNTABILITY .....</b>		<b>6</b>
<b>4. DATA GOVERNANCE AND RECORDS RETENTION .....</b>		<b>9</b>
<b>5. RESOURCE WASTE AND ACCOUNTABILITY .....</b>		<b>11</b>
<b>6. WHISTLEBLOWER PROTECTIONS.....</b>		<b>15</b>
<b>APPENDIX: SUPPLEMENTAL INFORMATION .....</b>		<b>17</b>
1. Safety, Security, and Preservation Management.....		17
2. Information and Cybersecurity Risk Management.....		17
3. Workforce Management and Accountability .....		17
4. Data Governance and Records Retention .....		18
5. Resource Waste and Accountability .....		18
6. Whistleblower Protections.....		19
<b>ACRONYMS AND ABBREVIATIONS .....</b>		<b>20</b>



# Inspector General

**DATE:** December 15, 2025

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

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

**SUBJECT:** Transmittal of the Fiscal Year 2025 Statement of Management Opportunities and Performance Challenges

I am pleased to transmit the Office of Inspector General's (OIG) Fiscal Year (FY) 2025 Statement of Management Opportunities and Performance Challenges (Statement) for inclusion in the Architect of the Capitol's (AOC's) Performance and Accountability Report. Consistent with oversight best practices identified in the Reports Consolidation Act of 2000<sup>1</sup> and Office of Management and Budget (OMB) Circular A-136,<sup>2</sup> this Statement provides an independent view of the most significant opportunities and challenges affecting the AOC's operations, internal controls, and overall mission performance.

All federal agencies face management challenges that require sustained attention, and the AOC is no exception. OIG presents this Statement from an independent oversight perspective, with the aim of supporting continuous improvement and strengthening the agency's effectiveness, accountability, and resilience. The assessment draws on OIG audits, evaluations, investigations, and other oversight activities conducted during the year as well as broader trends and patterns observed across multiple jurisdictions.

---

## Developments Impacting the AOC in FY 2025

In FY 2025, the AOC made meaningful progress in several areas that directly affect the agency's long-term capacity. Leadership stabilization, the filling of senior executive vacancies, and expanded recruitment partnerships enhanced organizational continuity. The agency also strengthened training, upskilling, and career development offerings, supporting workforce readiness and contributing to improvements across multiple mission areas.

At the same time, OIG oversight identified several conditions that continue to affect transparency, auditability, and operational efficiency. Property accountability challenges remain significant, with inconsistent practices and incomplete documentation impacting the agency's ability to safeguard resources. Nonstandardized recordkeeping and delays in producing documentation continue to hinder auditability and reduce visibility into potential waste, loss, or mismanagement.

---

<sup>1</sup> Public Law 106–531. Reports Consolidation Act of 2000. <https://www.congress.gov/106/plaws/publ531/PLAW-106publ531.pdf>.

<sup>2</sup> OMB. Circular A-136, Financial Reporting Requirements. <https://www.whitehouse.gov/wp-content/uploads/2025/04/OMB-Circular-No.-A-136.pdf>.

The agency's risk environment also evolved. The FY 2025 Targeted Risk Assessment identified a substantial increase in critical infrastructure risk due to aging systems and deferred maintenance. Cybersecurity challenges intensified as the AOC modernized its technology environment and has begun exploring incorporating artificial intelligence tools. The need for coordinated emergency preparedness and consistent physical security practices remained prominent, given the unique operating environment of the Capitol campus.

Despite these challenges, the AOC continues to carry out its mission under complex conditions — including fiscal constraints, heightened security demands, and the need to preserve a historic and heavily utilized campus. These developments provide important context for the management opportunities and performance challenges outlined in the attached Statement.

---

## **Management Opportunities and Performance Challenges**

Based on our oversight work, we have identified the following six areas that present significant management opportunities and performance challenges for the AOC:

- 1. Safety, Security, and Preservation Management**
- 2. Information and Cybersecurity Risk Management**
- 3. Workforce Management and Accountability**
- 4. Data Governance and Records Retention**
- 5. Resource Waste and Accountability**
- 6. Whistleblower Protections**

The attached Statement explains each challenge in detail, including the conditions observed, the associated risks for AOC operations and mission execution, and the progress the agency has reported in addressing these matters. The assessment also highlights cross-cutting factors, such as the effect of documentation deficiencies on auditability and the way infrastructure and cybersecurity challenges heighten vulnerability to operational disruptions.

OIG acknowledges the constructive steps the AOC has taken over the past year to strengthen its management practices and internal controls. Efforts to improve workforce development, enhance data and cybersecurity capabilities, advance physical security coordination, and refine property management reflect a commitment to continuous improvement. Sustained attention to these areas, along with focused action to address the challenges identified in this Statement, will help reinforce the AOC's effectiveness and organizational resilience.

As OIG identifies additional concerns through audits, inspections, evaluations, investigations, and management advisories, we will continue to provide timely recommendations to support the AOC's efforts to detect and prevent fraud, waste, abuse, and mismanagement. These recommendations are intended to enhance the efficiency and effectiveness of AOC programs and operations, ensure responsible stewardship of taxpayer resources, and reinforce the agency's capacity to fulfill its mission.

I appreciate the cooperation extended to OIG and value the professional engagement of your leadership team and staff during oversight activities. OIG remains committed to providing



objective information and recommendations that support the AOC's ability to "serve, preserve, and inspire" on behalf of Congress, the Supreme Court, and the American public. I look forward to continued constructive collaboration as the agency addresses the issues outlined in the Statement.



# 1. Safety, Security, and Preservation Management

Status: Renewed and Updated

Safety, security, and preservation management refers to the AOC's responsibility to "serve, preserve, inspire" while ensuring that construction, renewal, and daily operations protect the Capitol campus, its occupants, and its historical assets. This area also includes emergency preparedness, physical security, and consistency in applying safety codes and standards. Refer to the [Safety, Security, and Preservation Management](#) section in the appendix for relevant reports.

## Key Areas of Concern

Key areas of concern include physical security, emergency preparedness, and the management of critical infrastructure.

The Capitol campus continues to face elevated security threats that place people, property, and historical resources at risk. Physical security is essential to daily operations; however, safety considerations are not consistently integrated into routine decision-making.

In addition, the agency continues to confront complex demands associated with maintaining and preserving historic assets and managing an aging infrastructure portfolio. These challenges require coordinated planning, timely communication, and strong internal controls to ensure that safety, preservation, and mission needs remain in balance.

### ***Physical Security***

Physical security, like information technology (IT) security, depends on shared awareness and vigilance across an organization. However, physical security is not fully embedded in the AOC's day-to-day culture or operational routines. As a result, it remains a top-tier enterprise risk that directly affects the AOC's ability to fulfill its mission.

The AOC has a key role in the campus-wide security posture, particularly in managing suitability screening and badge processes for contractors. While security badge access itself is governed by the U.S. Capitol Police (USCP) for most entities, the AOC must ensure that contractor documentation, vetting, and access procedures are complete, timely, and accurate. OIG acknowledges progress made through the recent implementation of its Contractor Suitability Policy, but at present a comparable policy for AOC employees does not exist. Instead, the agency adheres to the approved Suitability Adjudicative Process SOP in administering the security badging program for AOC employees.

Situational awareness is central to mitigating potential physical security threats. The adage "see something, say something" is more than a reminder; it reflects the proactive posture required on a campus with unique security demands. Without consistent training and reinforcement, gaps in awareness can persist, especially as staff transition from remote or hybrid work environments back to regular campus operations.

OIG also notes that inconsistent sharing of threat assessment information among jurisdictions inhibits coordinated readiness.

While coordination with the Capitol Police Board and USCP is ongoing, the AOC's internal processes for communicating emerging threats and security concerns are not fully standardized.

### ***Emergency Preparedness***

Emergency preparedness remains a recurring challenge due to inconsistent implementation across the Capitol campus. Persistent threats—including suspicious packages, disruptions affecting public-facing jurisdictions, and localized security incidents—underscore the importance of clear, coordinated emergency response processes.

Despite the strong security presence of the USCP, some AOC employees work in areas with heightened exposure to external threats. These conditions can affect staff morale and well-being, as reflected in employee reliance on the AOC's Employee Assistance Program following certain incidents.

### ***Critical Infrastructure***

The AOC's infrastructure portfolio is aging, and deferred maintenance continues to grow. According to the FY 2025 Targeted Risk Assessment, critical infrastructure failure was identified as the agency's highest-rated risk, with its score increased from 16.2 in FY 2024 to 23.51 in FY 2025. This approximately 45 percent increase reflects both the scale of the challenge and the compounding effect of delayed investment.

Without adequate funding, the AOC faces challenges maintaining essential building systems and utilities, many of which are nearing or exceeding their expected lifecycle. Failures in these systems can disrupt congressional operations and

compromise both safety and preservation elements of the AOC's mission.

### ***Serve, Preserve, Inspire***

The AOC's mission to "serve, preserve, inspire" requires that construction, renewal, and maintenance activities honor the historic character of the Capitol campus while ensuring safe and functional operations. Preservation encompasses paper and electronic records, architectural drawings, models, product samples, and other materials that document the campus's unique heritage.

Timely development of preservation and archival policies remains essential. The AOC must ensure that historically significant materials are consistently identified, protected, and made accessible to support ongoing operational needs and institutional continuity. Adequate resources, including storage and archival expertise, are required to prevent loss, deterioration, or mismanagement of these one-of-a-kind records.

Balancing preservation needs with modernization goals also requires careful planning. The AOC must integrate heritage considerations early in project design and execution to ensure that historically significant spaces and materials are protected while still meeting evolving functional, safety, and accessibility requirements.





To manage these risks, the AOC must prioritize infrastructure needs through systematic assessments, clear planning documents, and strong coordination across jurisdictions. Transparent communication about funding requirements and risk implications remains critical to addressing this challenge.

The AOC also continues to use security awareness training to reinforce staff vigilance and support employees in identifying and responding to potential threats. Additionally, the agency participates in coordinated, campus-wide emergency exercises — such as internal threat and shelter-in-place drills — and produces After Action reports to guide process improvements.

## **Agency Progress**

OIG recognizes several ongoing efforts to strengthen safety, security, and preservation management. The agency has engaged actively with Capitol Police Board working groups and other campus partners to refine physical security governance and clarify management roles and responsibilities. These efforts are aimed at improving threat awareness, enhancing communication, and establishing more consistent internal processes.

Within preservation functions, the AOC has taken steps to support archival needs and consolidate guidance, although further work is needed to ensure historical materials are uniformly protected and accessible. Sustained attention to policy development and resource allocation will be essential as preservation demands grow alongside modernization and security requirements.

## 2. Information and Cybersecurity Risk Management

Status: Renewed and Updated

Information and cybersecurity risk management refers to the protection of sensitive information and technology assets in an environment marked by increasing cyber threats, public and private sector data breaches, and sophisticated attacks capable of disrupting critical IT services. Such disruptions could compromise data confidentiality, impede mission-critical functions, and affect the safety and security of the Capitol campus. Refer to the [Information and Cybersecurity Risk Management](#) section in the appendix for relevant reports.

### Key Areas of Concern

Key areas of concern include consistent application of Information Technology Division (ITD) policies across jurisdictions and emerging cybersecurity risks associated with the expanding use of artificial intelligence tools.

The AOC is responsible for the maintenance, development, and preservation of the Capitol campus and relies heavily on information systems to support its responsibilities. These systems often contain highly sensitive information, including detailed Capitol complex designs, emergency preparedness documents, and operational procedures. Because many systems are interconnected, vulnerabilities in one area can cascade across the network.

Cybersecurity remains a top-tier enterprise risk for the AOC. Threats continue to evolve, and the agency must ensure its policies, internal controls, and technology safeguards are consistently implemented to reduce exposure.

### *Policy and Implementation*

The AOC uses a variety of information systems to deliver its mission, and each system requires appropriate security controls, routine monitoring, and compliance with established ITD policies. While the

agency maintains cybersecurity directives, OIG oversight has found that these policies are not always applied consistently.

Cybersecurity attacks can disrupt network operations, limit access to essential services, and expose sensitive data. Advanced and persistent threats have the potential to cause significant harm, including damage to IT infrastructure and unauthorized disclosure of security-sensitive materials related to congressional continuity of operations.

Oversight activities have identified instances in which AOC personnel violated information security requirements, including ITD policy. In one case, the potential for a security breach could have been reduced had the agency confirmed receipt and review of the ITD Rules of Behavior. Variations in policy implementation across jurisdictions — combined with incomplete documentation of cybersecurity processes — continue to create gaps that adversaries could exploit.

OIG continues to evaluate emerging risks and vulnerabilities and to document potential impacts to AOC systems and operations.

## ***Information Security Modernization***

The AOC must manage heightened cyber risk while supporting Congress, which increases its visibility as a potential target for hostile actors. Broader federal IT modernization requirements — including movement toward Zero Trust Architecture — demand sustained investment in technology, process redesign, and workforce readiness.

The agency's exposure to cyber threats is expanding as operations increasingly depend on interconnected systems, cloud-based tools, and artificial intelligence-enabled capabilities. These advancements offer important benefits but also raise new security considerations. Without strong governance, established control frameworks, and consistent oversight, new technologies may increase the risk of malicious activity, data inaccuracies, or unauthorized exposure of sensitive information.

Effective modernization requires close coordination across jurisdictions, reliable documentation of system configurations and vulnerabilities, and prioritized remediation of known weaknesses. A comprehensive, agencywide cybersecurity strategy will support resilience and reduce the risk of operational disruptions, data breaches and reputational harm.

## **Agency Progress**

The AOC has taken several steps to strengthen its information security controls and risk management practices. It recently updated its overarching cybersecurity policy, clarifying requirements and responsibilities for safeguarding information systems under the AOC's authority or control.

Additional improvements include launching an executive cybersecurity dashboard, enhancing processes for identifying and assessing IT weaknesses, and improving tracking of remediation activities. The AOC continues to make progress toward implementing Zero Trust Architecture principles, including the refinement of identity, access management, and monitoring capabilities.

While these efforts demonstrate a commitment to strengthening the agency's cybersecurity posture, consistent implementation across jurisdictions remains essential. Sustained investment in technology infrastructure, risk management processes, and workforce education are critical to meeting the evolving cybersecurity challenges facing the AOC.

### 3. Workforce Management and Accountability

Status: Renewed and Updated

Workforce management and accountability encompasses a wide range of personnel-related activities, including workforce planning (e.g., hiring, retention, and training), employee benefits and services, payroll administration, and employee and labor relations. These functions are fundamental to the AOC's ability to execute its mission effectively. Refer to the [Workforce Management and Accountability](#) section in the appendix for relevant reports.

#### Key Areas of Concern

Key areas of concern related to workforce management and accountability include recruitment and retention, equitable hiring practices, and recurring employee misconduct.

For more than two decades, the Government Accountability Office (GAO) has identified strategic human capital management as a governmentwide high-risk area.<sup>3</sup> While this area is no longer the AOC's highest-rated enterprise risk, the agency continues to experience shortages in critical skill areas.

As in previous years, OIG has observed instances of employee misconduct and inconsistent or incorrectly applied accountability measures. If these conditions remain unaddressed, they may contribute to a culture of distrust and lower morale. Despite increased employee education efforts, noncompliance with AOC policies continues, especially in labor relations and management practices.

#### ***Recruiting and Retaining a Highly Skilled Workforce***

The AOC continues to face challenges recruiting and retaining a diverse, highly skilled workforce. Contributing factors

include complex and sometimes lengthy hiring processes, an aging workforce, and the need to attract and retain specialized trades. These challenges are compounded by a federal compensation structure that may not be competitive with broader labor market conditions.

A strong recruitment and retention strategy is essential to maintaining institutional knowledge and service quality. The AOC reports having expanded recruitment efforts through strategic partnerships and notes a 6.6 percent agencywide decrease in vacancy rates, as of June 2025, with all senior leadership positions filled. This represents a notable improvement over the conditions highlighted in FY 2024. However, gaps persist, largely due to limited staffing and funding to support recruitment efforts to address current human capital needs.

To strengthen its position, the AOC should continue monitoring workforce trends to anticipate talent needs, strengthen strategic partnerships, fully leverage available hiring flexibilities, and pursue innovative approaches to recruiting, developing, and retaining a skilled, motivated, and diverse workforce.

<sup>3</sup> GAO. 2023. *High Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully*

Address All Areas, GAO-23-106203.  
<https://files.gao.gov/reports/GAO-23-106203/index.html>.



## ***Equitable Hiring Practices***

Staff continue to raise concerns about the fairness and transparency of hiring practices. OIG receives complaints alleging that less-qualified candidates are selected (including into managerial positions) based on prior working relationships with senior staff or hiring officials, while more experienced internal candidates are not advanced. The perception that supervisory positions are prioritized over nonsupervisory roles needed for day-to-day operations contributes to concerns about equity and organizational effectiveness.

These reports also highlight allegations related to direct-hire actions and limited opportunities for internal advancement. Some employees report frustration over the lack of clear pathways for upward mobility. In several matters, OIG inquiries were impeded because supporting records — such as résumés, vacancy announcements, or other hiring documentation — were incomplete or not maintained. While not all complaints warrant full investigations and many are referred to the AOC for further review, the volume and nature of these concerns underscore ongoing perceptions of favoritism, nepotism, and questionable qualification determinations.

The AOC is encouraged to review its policies, practices, and procedures to identify and address potential biases or barriers that may prevent qualified employees or applicants from being hired or promoted.

## ***Employee Misconduct and Inconsistencies in Accountability Practices***

Workplace compliance is necessary to safeguard employees, support achievement of strategic and operational goals, and

maintain a productive environment. OIG continues to observe inconsistent application of, and noncompliance with, AOC policies and orders across multiple jurisdictions and offices. Much of the noncompliance relates to labor relations and management practices.

OIG notes that, in some instances, employees may be unclear about their responsibilities and obligations under AOC policies and orders. Prior management opportunities and performance challenges have also documented differences in how administrative actions are applied following substantiated misconduct, both across and within jurisdictions. For similar violations, outcomes can vary significantly.

As reports of misconduct and noncompliance continue despite enhanced training and communication, there is growing concern that the AOC's reputation and workplace culture could negatively affect recruitment and retention. Leadership plays a key role in shaping agency culture, and as the AOC advances its efforts to manage cultural and reputational risk, OIG encourages continued attention to consistent, ethical leadership and practices that help promote accountability at all levels.

## ***Agency Progress***

While the AOC's Human Capital Management Division recently conducted a Wage Grade Compensation Study to understand and help address pay inequities and retention of skilled trade workers, a definitive implementation timeline has not been established. While competitive salaries are essential, other factors are equally if not more important for retaining talent. Opportunities for career growth, a positive organizational culture, and



work-life balance are crucial for keeping employees engaged in their roles. The AOC recognizes these additional factors and has expanded its training offerings and established several transitional career development initiatives, including upskilling and trade exploration programs as well as opportunities for certification and mastery within select fields.

The agency's goal is to provide a comprehensive employee development framework to ensure the agency has exceptional leaders ready to seamlessly step into new opportunities, supporting efficient knowledge management and retention of critical leadership talent. According to AOC, in FY 2025, it processed 351 promotions to fill vacant positions. By investing in the growth and development of employees, the AOC seeks to ensure organizational readiness through a structured talent pipeline.



## 4. Data Governance and Records Retention

Status: Renewed and Updated

Data governance and records retention refers to the consistent application of procedures for recording transactions, communications, and significant events so that documentation is complete, reliable, and readily available for examination. Refer to the [Data Governance and Records Retention](#) section in the appendix for relevant reports.

### Key Areas of Concern

Key areas of concern include nonstandardized documentation practices and ongoing data quality issues.

While some improvements have been observed, the AOC continues to face challenges in applying uniform documentation procedures across jurisdictions. OIG requests frequently result in delayed, incomplete, or missing records, which prolongs oversight work and, at times, requires rework. These conditions impair transparency; limit insight into potential fraud, waste, abuse, and mismanagement; and elevate the agency's risk profile.

Data integrity and timely availability of information remain persistent enterprise-wide concerns, affecting the AOC's ability to support data-driven decision-making and maintain reliable operational records.

#### ***Nonstandardized Documentation Practices***

Documentation practices vary widely across AOC jurisdictions and offices. Records are not always maintained with the level of detail or organization necessary to support transactions, management decisions, or third-party review. The absence of a consistent, agencywide approach to documenting the lifecycle of transactions — from initiation through final disposition — continues to undermine auditability.

OIG's audit of the Senate Furniture Program illustrates these challenges. Ineffective inventory management processes led to inaccurate records, and insufficient documentation limited OIG's ability to locate assets and verify compliance with accountability practices. These weaknesses demonstrate the need for documentation standards that apply uniformly throughout the lifecycle of a transaction or event, supported by clear roles, responsibilities, and points of contact.

OIG has also encountered difficulties obtaining complete ITD records for departing employees unless requests are made immediately upon separation. While ITD has updated some retention practices and made progress in preserving certain records, resource constraints and the need for specific software capabilities continue to present challenges.

Similar concerns arise in procurement documentation. Despite recent updates to the contracting manual, some contract files remain incomplete or inconsistent across systems. Thorough documentation is essential for effective oversight, ensuring compliance with regulations, preventing unnecessary costs, and supporting informed management review.



## ***Data Quality***

High-quality data are fundamental to mission execution and organizational efficiency. A strong data governance framework supports collaboration, transparency and informed decision-making while helping to mitigate security risks through controlled access and appropriate handling of sensitive information.

The AOC continues to rely on multiple disparate systems that are not fully integrated, limiting its ability to generate accurate, consolidated reporting and insights. This fragmentation contributes to data silos, inefficiencies, and inconsistencies in how information is captured and used across the enterprise.

The rapid expansion of artificial intelligence tools further elevates the importance of sound data governance. Effective use of these technologies depends on access to accurate, reliable data and staff capacity to analyze and apply it appropriately.

## **Agency Progress**

Although several previously identified deficiencies have been addressed, adherence to policy remains inconsistent across jurisdictions, and practices continue to vary. Ensuring uniform application of existing standards will be critical to achieving sustained improvement.

The AOC reports progress toward acquiring a data cataloging and governance system that, once fully implemented, should enhance the agency's ability to manage, classify, and access enterprise data. This investment is expected to improve the timeliness, reliability, and usability of information across the organization and strengthen the foundation for data-driven decision-making.

In FY 2025, AOC issued Order 8-6: Data Management Policy, assigning responsibility to system owners for ensuring the accuracy and quality of data entered and maintained within their systems.



## 5. Resource Waste and Accountability

Status: Renewed and Updated

Resource waste and accountability refers to the extravagant, careless, or needless expenditure of AOC funds or the consumption of AOC property that results from operational and programmatic redundancies, deficient practices, weak systems, ineffective controls, or poor decisions. Intent is not necessarily a factor in defining waste. This challenge area also encompasses the absence of comprehensive accountability standards governing the wasteful use of government resources. Refer to the [Resource Waste and Accountability](#) section in the appendix for relevant reports.

### Key Areas of Concern

Key areas of concern related to waste and accountability include inconsistently applied policies and policy noncompliance, the impact of these conditions on accountability, and internal controls and the continued need for a working capital fund to reduce fragmentation and duplication in agency processes.

The AOC has an obligation to the American taxpayers to pursue cost-effective and responsible ways to carry out its mission. Despite this responsibility, OIG work continues to identify a pattern of wasteful practices across multiple programs and functions. A strong internal control system should provide reasonable assurance of efficient operations and compliance with laws and regulations; however, persistent reports of waste, abuse, and policy noncompliance weaken that system. In numerous instances, OIG has substantiated complaints involving wasteful actions and behaviors that occurred repeatedly and without appropriate consequence.

Relatedly, OIG has observed ongoing inconsistencies in the application of administrative actions following findings of employee misconduct. These differences occur both across and within jurisdictions and contribute to a culture in which

recurrent waste of government and taxpayer resources can become normalized rather than promptly corrected.

#### ***Inconsistent Application of Policy***

OIG continues to observe inconsistent application of, and noncompliance with, AOC policies and orders across many jurisdictions and offices. Policy compliance is essential to protect employees, achieve strategic and operational goals, and ensure that taxpayer resources are managed responsibly.

Ambiguities in AOC policy contribute to this environment. Several policies lack a clear definition of waste, do not explicitly assign or require specific roles and responsibilities, and are not supported by consistent record-keeping practices. These weaknesses align with other documentation and data challenges discussed elsewhere in this Statement. Additionally, AOC policies and orders do not include comprehensive accountability standards addressing wasteful use of government resources.

In multiple investigations, OIG has identified wasteful actions for which the consequences did not align with the seriousness of the conduct or the



requirements of policy. Examples include falsification of records, unreported outside employment, attempts to circumvent established processes, and inappropriate relationships. In some cases, employees engaged in these behaviors without facing meaningful remedial or disciplinary action.

The AOC's discipline matrix also remains silent on noncooperation with OIG, even though such conduct impedes effective oversight and reduces transparency. The absence of clear consequences for noncooperation can discourage candor, delay investigations, and weaken the agency's ability to respond to issues in a timely, well-informed manner.

Given these conditions, OIG strongly reiterates that AOC policies and orders must be clearly understood, readily accessible, frequently communicated, and consistently applied throughout the agency. Doing so is critical to reducing the risk of fraud, waste, and mismanagement; mitigating legal and safety risks; and improving the effectiveness and efficiency of AOC programs and operations.

### ***Inventory Accountability and Controls***

Operational inefficiency and ineffectiveness can lead directly to asset mismanagement and increase the agency's vulnerability to waste, loss, or theft. Weaknesses in inventory accountability and controls remain a significant concern.

An OIG audit of the Senate Furniture Program found that policies, procedures, and processes for acquiring, safeguarding, transferring, and disposing of furniture were inefficient and ineffective. As a result, inventory costs were overstated, records were inaccurate, and staff were unable to locate or safeguard furniture or provide

adequate supporting documentation. These conditions increase the risk of undetected loss or theft and reduce confidence in reported inventory balances.

Across the AOC, accountable property is not consistently defined or standardized. Jurisdictions determine what property they consider accountable, and OIG continues to receive reports of "lost" items on a recurring basis. While jurisdictions have different missions and operational needs, excessive discretion in determining what must be tracked can create gaps in inventory management and control. There is an elevated risk that mission-critical, nonconsumable property — essential items that are used frequently and not easily discarded — is not consistently documented or monitored.

This challenge extends to nonaccountable property, which is not required to be reported in the property management system. Some mission-critical items may therefore be treated as nonaccountable and remain untracked. The lack of a clear and consistently applied distinction between accountable and nonaccountable property makes it difficult to hold employees responsible for misplaced or missing assets. In some cases, OIG has found that there is no documentation at all for missing items or that months have passed since an item was last recorded or seen.

At a minimum, the agency must update and implement procedures that increase accountability; ensure property is properly safeguarded; and prevent unauthorized use, theft, and loss of inventory. Enhanced monitoring and tracking would help reduce these negative outcomes and improve the overall control environment.



In a FY 2023 follow-up evaluation of the AOC's inventory accountability and controls, OIG recommended the agency update its policy on the personal property management lifecycle by clarifying dollar thresholds for accountable property and develop more robust accountability procedures to reduce the risk of property mismanagement. Although completion of this work was originally anticipated in FY 2024, the policy remains in draft status and the underlying challenges persist.

In a more recent evaluation of the AOC's Supply Chain Risk Management (SCRM) process, the OIG determined that the agency has not established consistent governance of SCRM. The absence of centralized oversight increases the potential for waste and undermines accountability. Without a unified framework and standard assessment protocols, the AOC is more vulnerable to procuring high-risk goods and services, including counterfeit or compromised products that could affect mission-critical systems. It also becomes more difficult to ensure that procurement decisions are both cost-effective and security conscious. As a result, the agency faces heightened risk of duplicative purchasing, inefficient sourcing and limited visibility into how funds are allocated and managed.

AOC senior leaders should acknowledge these risks, set clear expectations for stewardship of resources and actively address wasteful practices. Strong internal controls, well-defined standard operating procedures, effective training and frequent communication collectively demonstrate leadership's commitment to accountability and risk mitigation.

## ***Working Capital Fund***

Management of construction projects and other programs that span multiple appropriations presents challenges and risks that are not typical for agencies with more centralized funding structures. While thorough planning and design can mitigate some of these issues, unforeseen conditions, schedule changes, and evolving security or infrastructure needs can increase costs and create inefficiencies.

In the absence of a working capital fund, the AOC must manage shared services and cross-cutting activities through decentralized arrangements. This can lead to operational and programmatic redundancies, fragmented decision-making, and limited visibility into the full cost of services. Without a central mechanism to manage common support activities, the agency is more likely to experience inefficiencies, waste, and duplication of effort that could be reduced through more coordinated, centralized funding and management.

## **Agency Progress**

The agency has indicated that a revised disciplinary policy is under development that is intended to align with best practices, streamline the handling of disciplinary cases, and reinforce fairness and consistency. OIG recognizes the substantial number of policies that have been updated or revised over the past year and encourages the AOC to focus equally on ensuring that these changes are fully understood and consistently applied throughout the organization. Improved awareness and implementation can help reduce misconduct and strengthen the internal control environment.

The Acquisition and Material Management Division is actively collaborating with jurisdictions to refine processes for tracking and maintaining AOC property. As part of these efforts, the AOC conducted an organization-wide property assessment to identify unused or excess items for proper

disposition. Following this assessment, offices and jurisdictions turned in 58 pieces of excess property totaling \$421,237.48. These actions represent positive steps toward improving inventory management, reducing waste, and enhancing accountability for government resources.



## 6. Whistleblower Protections

Status: Renewed and Updated

Whistleblower protections refers to leadership's responsibility to maintain a safe workplace where employees can report concerns about fraud, waste, abuse, or misconduct without fear of reprisal. This responsibility includes ensuring that employees understand their rights, have access to confidential reporting mechanisms, and can raise concerns without exposure to retaliation. Refer to the [Whistleblower Protections](#) section in the appendix for relevant reports.

### Key Areas of Concern

Key areas of concern related to whistleblower protections include safeguarding employees from retaliation and strengthening internal processes that support reporting.

Because the AOC is a legislative branch agency, its employees are not covered by the Whistleblower Protection Act. Instead, protections arise under the Congressional Accountability Act, which prohibits employing offices from intimidating, retaliating against, or discriminating against employees who report allegations of wrongdoing. The effectiveness of these protections depends on the AOC's internal procedures and the degree to which leadership fosters a culture that encourages reporting.

OIG continues to receive allegations of fraud, waste, and abuse through its independent hotline. While increased reporting reflects employees' willingness to raise concerns, many individuals still express hesitation due to fears of reprisal or uncertainty about the protections available. Ensuring that employees feel safe to speak up is essential to identifying misconduct early, promoting accountability, and strengthening the integrity of AOC operations.

### *Availability of Protection*

Although OIG treats all allegations with the utmost seriousness and confidentiality, some reporting parties continue to express limited confidence in the protections available to them. Employees have raised concerns about the potential for retaliation after reporting violations to OIG or through internal channels. The AOC has a responsibility to reinforce that employees who raise legitimate concerns will not face adverse consequences for doing so.

As noted in Section 5, Resource Waste and Accountability, the AOC's discipline matrix does not currently address violations involving noncooperation with OIG. This omission may discourage full participation in investigations and reduces transparency in situations where accountability is necessary. Establishing consistent expectations for cooperation would enhance oversight effectiveness and reinforce a culture of integrity.

OIG has observed an increase in the volume of complaints in recent years. While this rise may reflect improved awareness of reporting avenues, it also underscores the importance of having clear, enforceable protections in place. According to the AOC's FY 2025 targeted risk assessment, whistleblower protections have emerged as





a developing risk area for the agency. This recognition provides an important opportunity for the AOC to assess its policies, strengthen protections and address internal barriers that may inhibit reporting.

Though formal statutory whistleblower protections would require legislative action, the AOC can take steps within its existing authority to strengthen its internal framework. These steps include expanding training on whistleblower rights, reinforcing nonretaliation policies, ensuring confidentiality, and setting clear expectations for leadership behavior. Other legislative branch agencies have implemented similar measures to strengthen reporting pathways and can serve as a model for enhancing AOC practices.

## APPENDIX: SUPPLEMENTAL INFORMATION

---

The following sections list reports relevant to each subject opportunity/challenge.

### 1. Safety, Security, and Preservation Management

- *White Paper on the Research of the Architect of the Capitol's Management of Deferred Maintenance and Capital Renewals* ([OIG-AUD-2024-04](#))
- *Architect of the Capitol Targeted Risk Assessment Report FY 2025* (Not Releasable to Public)
- *Evaluation of the Architect of the Capitol's Security Badging Program* ([2022-0001-IE-P](#))
- *Evaluation of the Architect of the Capitol's Safety Inspection Program* ([2022-0004-IE-P](#))
- *Architect of the Capitol Office of Inspector General Organizational Risk Assessment FY 2023* (Not Releasable to Public)

### 2. Information and Cybersecurity Risk Management

- *Evaluation of the Architect of the Capitol's Implementation of Information Security Modernization for Fiscal Year 2024* ([2024-004-IE-P](#))
- *Evaluation of the Architect of the Capitol's (AOC's) Implementation of the Federal Information Security Modernization Act of 2014 (FISMA), Fiscal Year 2022* ([2022-0005-IE-P](#))
- *Evaluation of the Information Technology Division's Inventory Accountability and Controls* ([2022-0002-IE-P](#))
- *Allegations of Forgery and Security Violations Related to the Security of Personally Identifiable Information (PII)* ([2024-0006-INVI-P](#))
- *Misuse of Government Issued iPhone* ([2024-0001-INVI-P](#))
- *Misuse of Government Issued iPhone* ([2024-0017-INVI-P](#))

### 3. Workforce Management and Accountability

- *Inequitable Hiring Practices*: 2025-0004-INVC-P; 2025-0005-INVC-P; 2025-0010-INVC-P; 2025-0012-INVC-P; 2025-0013-INVC-P; 2025-0037-INVC-P; 2025-0005-INVR-P (Not Releasable to Public)
- *Unreported Outside Employment and Allegations of Paycheck Protection Program (PPP) and Economic Injury Disaster Loan (EIDL) Fraud* ([2024-0015-INVI-P](#))
- *Theft of Government Property* ([2023-0016-INVI-P](#))
- *Former Architect of the Capitol (AOC) Employee Committed Destruction of Government Property Inside Library of Congress Adams Building* ([2024-0004-INVI-P](#))
- *Inappropriate Relationship, Retaliation and Truthfulness* ([2025-0003-INVI-P](#))
- *Allegation of Malingering* ([2025-0005-INVI-P](#))
- *Fraudulent Medical Documentation* ([2024-0019-INVI-P](#))
- *Time and Attendance Fraud* ([2024-0023-INVI-P](#))
- *Misuse of Government Equipment* ([2025-0002-INVI-P](#))
- *Paycheck Protection Program (PPP) and Economic Injury Disaster Loan (EIDL) Fraud* ([2024-0005-INVI-P](#))
- *Fiscal Year 2023 Financial Statements Audit Management Letter* ([OIG-AUD-2024-02](#))



- *The Architect of the Capitol Human Capital Management Program Evaluation* ([2023-0003-IE-P](#))
- *Follow-Up Evaluation of the Congressional Request for Architect of the Capitol's Response to Sexual Harassment* ([OIG-FLD-2022-01](#))
- *Architect of the Capitol Office of Inspector General Semiannual Report to Congress* ([24-1](#))
- *Outside Employment While on COVID-19 Administrative Leave* ([2023-0004-INVI-P](#))
- *Inappropriate Romantic Relationship Involving a Senior Rated (SR) Employee and a Subordinate Supervisor* ([2023-0005-INVI-P](#))
- *Unreported Outside Employment and Employment of Subordinate Architect of the Capitol (AOC) Employees* ([2023-0009-INVI-P](#))
- *Alleged Violations of Contract Protocol in Hiring of Yoga Instructor* ([2023-0012-INVI-P](#))
- *False Medical Documentation* ([2023-0015-INVI-P](#))
- *Misuse of Government Issued iPhone* ([2024-0001-INVI-P](#))
- *Misuse of Government Issued iPhone* ([2024-0017-INVI-P](#))
- *Office of Inspector General (OIG) Management Advisory Report – Clear, Consistent and Uniform Application of Architect of the Capitol (AOC) Policy* ([2023-0006-INVM-P](#))
- *Architect of the Capitol (AOC) Implementation of the Pregnant Workers Fairness Act* ([2024-0001-INVM-P](#))
- *Architect of the Capitol Office of Inspector General Organizational Risk Assessment FY 2023* (Not Releasable to Public)
- *Architect of the Capitol Targeted Risk Assessment Report FY 2025* (Not Releasable to Public)

#### **4. Data Governance and Records Retention**

- *Audit of the Architect of the Capitol's Senate Furniture Program* ([OIG-AUD-2025-03](#))
- *Follow-up Evaluation of the Architect of the Capitol's Compliance with the Government Purchase Card Program* ([OIG-FLD-2025-01](#))
- *AOC Locality Pay for Remote Employees* ([2023-0047-INVC-P](#))
- *Evaluation of the Architect of the Capitol's Contracting Officer and Contracting Officer's Representative Oversight* ([2023-0002-IE-P](#))
- *The Architect of the Capitol Human Capital Management Program Evaluation* ([2023-0003-IE-P](#))
- *Audit of the Architect of the Capitol's Construction Division* ([OIG-AUD-2024-06](#))
- *Follow-Up Evaluation of the Congressional Request for Architect of the Capitol's Response to Sexual Harassment* ([OIG-FLD-2022-01](#))
- *Follow-Up Evaluation of the Architect of the Capitol's Inventory Accountability and Controls* ([OIG-FLD-2023-01](#))
- *Follow-Up Evaluation of the Architect of the Capitol Data Center* ([OIG-FLD-2024-01](#))
- *Audit of the Architect of the Capitol's Senate Furniture Program* ([OIG-AUD-2025-03](#))

#### **5. Resource Waste and Accountability**

- *Audit of the Architect of the Capitol's Senate Furniture Program* ([OIG-AUD-2025-03](#))
- *Theft of Government Property* ([2023-0016-INVI-P](#))
- *ROI 2023-0010-INVI-P* (not published)

- *Overtime Abuse* ([2024-0013-INVI-P](#))
- *Evaluation of the Architect of the Capitol's Supply Chain Risk Management* ([2024-0003-IE-P](#))
- *Follow-Up Evaluation of the Architect of the Capitol's Inventory Accountability and Controls* ([OIG-FLD-2023-01](#))
- *AOC Locality Pay for Remote Employees* ([2023-0047-INVC-P](#))
- *Alleged Violations of Contract Protocol in Hiring of Yoga Instructor* ([2023-0012-INVI-P](#))
- *Architect of the Capitol—Proposal for Establishment of a Working Capital Fund* ([B-328065](#))
- *Evaluation of the Architect of the Capitol's Fleet Management Program* ([2021-0001-IE-P](#))

## **6. Whistleblower Protections**

- 2025-0003-INVC-P, 2025-0006-INVC-P, 2025-0010-INVC-P, 2025-0012-INVC-P, 2025-0019-INVC-P, 2025-0025-INVC-P, 2025-0026-INVC-P, 2025-0027-INVC-P, 2025-0028-INVC-P, 2025-0031-INVC-P, 2025-0033-INVC-P, 2025-0037-INVC-P (Not Releasable to Public)
- Recommendations for Improvements to the Congressional Accountability Act, ([118th Congress, Office of Congressional Workplace Rights](#))



# ACRONYMS AND ABBREVIATIONS

---

AOC	Architect of the Capitol
FY	fiscal year
GAO	Government Accountability Office
IT	information technology
ITD	Information Technology Division
OIG	Office of Inspector General
OMB	Office of Management and Budget
SCRM	Supply Chain Risk Management
USCP	U.S. Capitol Police



