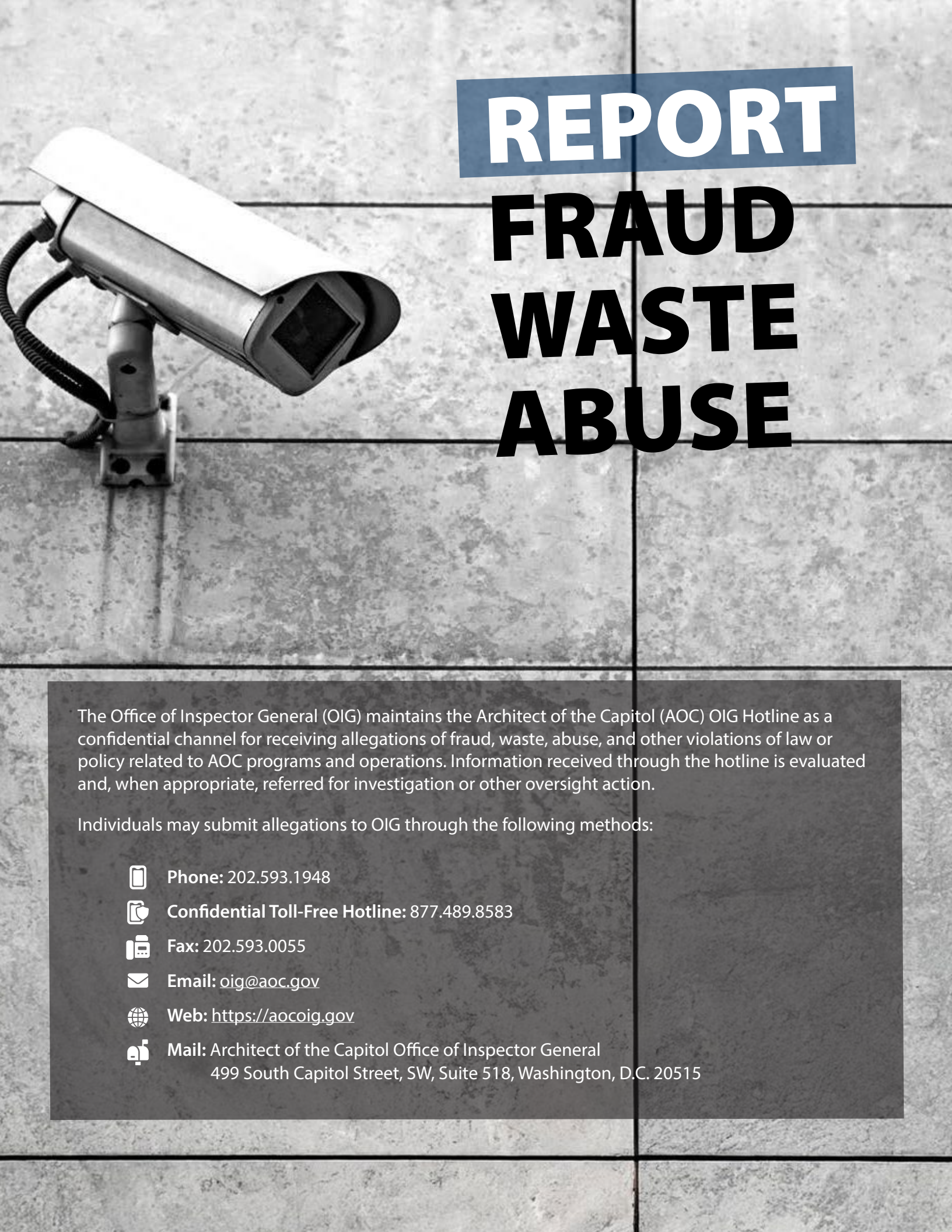


ARCHITECT OF THE CAPITOL
OFFICE OF INSPECTOR GENERAL

STATEMENT OF MANAGEMENT OPPORTUNITIES AND PERFORMANCE CHALLENGES

FISCAL YEAR 2026



REPORT FRAUD WASTE ABUSE

The Office of Inspector General (OIG) maintains the Architect of the Capitol (AOC) OIG Hotline as a confidential channel for receiving allegations of fraud, waste, abuse, and other violations of law or policy related to AOC programs and operations. Information received through the hotline is evaluated and, when appropriate, referred for investigation or other oversight action.

Individuals may submit allegations to OIG through the following methods:

- **Phone:** 202.593.1948
- **Confidential Toll-Free Hotline:** 877.489.8583
- **Fax:** 202.593.0055
- **Email:** oig@aoc.gov
- **Web:** https://aocoig.gov
- **Mail:** Architect of the Capitol Office of Inspector General
  499 South Capitol Street, SW, Suite 518, Washington, D.C. 20515

Memo From the Inspector General



DATE: November 16, 2026

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 2026 Statement of Management Opportunities and Performance Challenges



Luiz A. Santos, CFE, PMP
Inspector General

I am pleased to transmit the Architect of the Capitol (AOC) Office of Inspector General (OIG) Fiscal Year (FY) 2026 Statement of Management Opportunities and Performance Challenges (Statement) for inclusion in the AOC's Performance and Accountability Report. Consistent with oversight best practices identified in the Reports Consolidation Act of 2000[1] and Office of Management and Budget (OMB) Circular A-136,[2] 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 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 in recent years as well as broader trends and patterns observed across multiple jurisdictions.

DEVELOPMENTS IMPACTING THE AOC IN FY 2026

In FY 2026, the AOC addressed several existing risks, including strengthening the agency's cybersecurity posture and risk management practices. Of particular note, the AOC introduced a more structured project prioritization process that will enable leadership to reprioritize resources as operational conditions and funding availability evolve. Further, the AOC implemented numerous cybersecurity recommendations from recent OIG work. AOC leadership's ongoing commitment to corrective action is evident: the AOC implemented 32 recommendations in FY 2026, and just 17 OIG recommendations have remained open for more than 1 year. The AOC continually improves in response to oversight work.

[1] Public Law 106–531. Reports Consolidation Act of 2000. https://www.congress.gov/106/plaws/publ531/PLAW-106publ531.pdf.
[2] OMB. Circular A-136, Financial Reporting Requirements. https://www.whitehouse.gov/wp-content/uploads/2025/04/OMB-Circular-No.-A-136.pdf.

Concurrently, OIG oversight identified several challenges facing the AOC. The nature of the AOC's mission and responsibility involve mitigating risks related to safety, security, and cybersecurity, and OIG provided recommendations to support the AOC in navigating those risks. Additionally, our work has identified gaps in data governance and records retention, particularly as it relates to procurement, that continue to affect data integrity, auditability, and operational efficiency. Maintaining complete, accurate data and records on AOC programs and contracts continues to be an ongoing issue absent clear and consistently applied data quality and record maintenance policies.

Additionally, OIG notes the increase in critical infrastructure risk due to assets exceeding their useful life expectancy and inconsistent funding, which in turn has resulted in a significant deferred maintenance backlog. OIG recently initiated work in this area to add value to the AOC's efforts to address these challenges.

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 this Statement.

MANAGEMENT OPPORTUNITIES AND PERFORMANCE CHALLENGES IN FY 2026

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 and Security
2. Information and Cybersecurity Risk Management
3. Workforce Management and Accountability
4. Data Governance, Records Retention, and Procurement
5. Critical Infrastructure, Deferred Maintenance, and Preservation Management
6. Whistleblower Protections

This 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. It 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. As described throughout, the AOC has made strides — including by addressing OIG recommendations — in emergency preparedness, suitability, cybersecurity, and human capital management. Additionally, the agency is engaged in matters involving discipline and employee misconduct. Challenges remain, but OIG remains committed to supporting the AOC as it navigates these risks through independent, objective oversight.

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.

Table of Contents

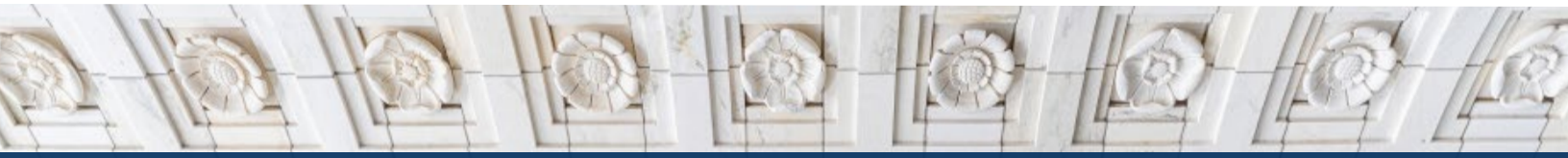
Memo From the Inspector General i

MANAGEMENT OPPORTUNITIES AND PERFORMANCE CHALLENGES 1

1. Safety and Security 2
2. Information and Cybersecurity Risk Management 5
3. Workforce Management and Accountability 8
4. Data Governance, Records Retention, and Procurement 11
5. Critical Infrastructure, Deferred Maintenance, and Preservation Management 14
6. Whistleblower Protections 17

APPENDICES 19

Appendix A. Supplemental Information 20
Appendix B. List of Acronyms Used 22



Inspector General Act

The Architect of the Capitol Inspector General Act of 2007, Title 2 United States Code §1808, established the Office of Inspector General as an independent, objective office within the Architect of the Capitol (AOC). It applies certain sections of the Inspector General Act of 1978 that detail the Inspector General's duties and authorities and establish important protections for AOC employees and responsibilities for the AOC.

Vision

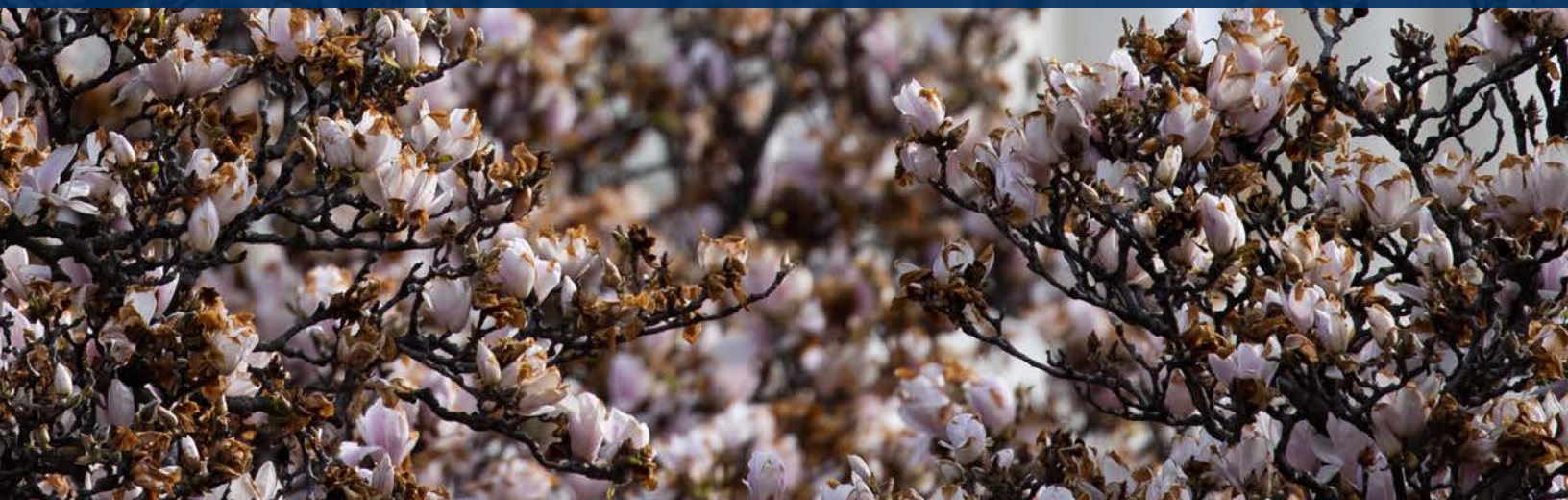
Be a trusted and independent oversight partner that drives accountability, safeguards AOC resources, and supports the enduring institutions that represent American democracy.

Mission

Provide independent, objective oversight that promotes integrity and accountability, improves performance, and safeguards the AOC's stewardship of historic facilities, infrastructure, and resources in service to Congress, the Supreme Court, and the American people.



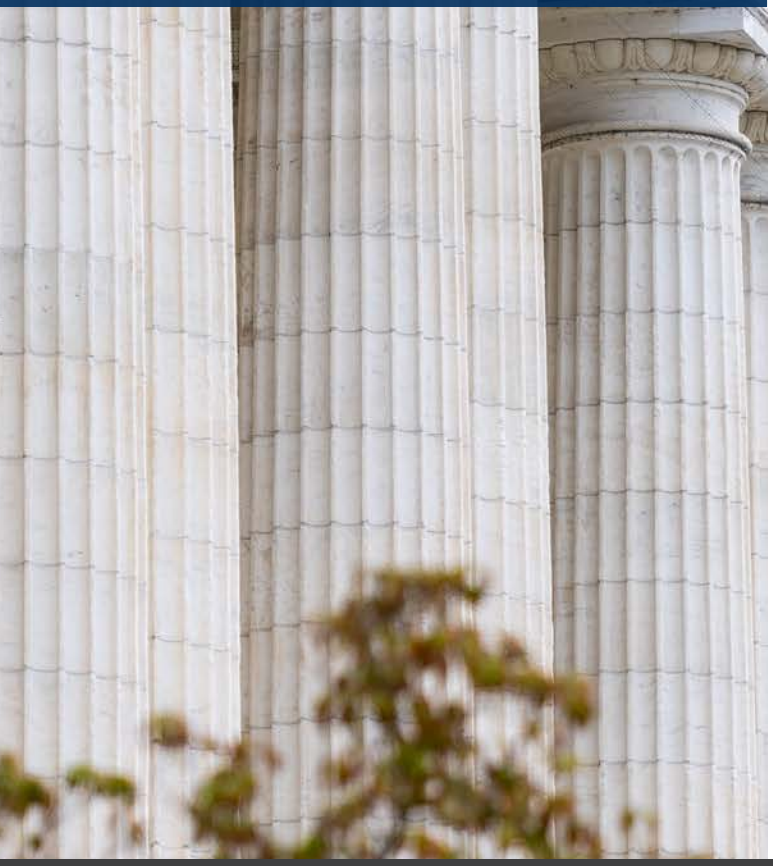
Management Opportunities and Performance Challenges



1. SAFETY AND SECURITY

Status

RENEWED AND UPDATED



Safety and security refers to the AOC's responsibility to "serve, preserve, and inspire" while ensuring that daily operations protect the Capitol campus, its occupants, and its assets. This area also includes physical security, emergency preparedness, and consistency in applying safety and security practices.

Since 2022, OIG has issued 8 reports and made 22 recommendations pertaining to safety and security. Of these, seven recommendations remain open. Refer to the Safety and Security section in Appendix A for a complete list of relevant reports.

KEY AREAS OF CONCERN

Key areas of concern include: (1) physical security, (2) emergency preparedness, and (3) employment suitability. These concerns are highlighted to strengthen the agency's safety and security posture in furtherance of the AOC's mission to serve Congress and the Supreme Court, preserve America's Capitol, and inspire memorable experiences.

Physical Security

Physical security encompasses the protection of people, property, assets, and information from threats, damage, and/or loss and depends on shared awareness and vigilance across an organization. In 2025, the AOC highlighted physical security and life safety as top priorities partly due to heightened risk requiring consistent monitoring of evolving threat environments. Challenges in improving physical security continue to exist in the AOC that directly affect the AOC's ability to fulfill its mission.

Within the last year, OIG observed an increase in law enforcement and security-related incidents involving AOC employees, including thefts, criminal violations, and fraud. One underlying issue could come from inconsistent awareness of security responsibilities. In FY 2027, OIG plans to conduct expanded fraud awareness training and outreach for AOC staff.

Situational awareness is an important component of physical security when people can distinguish between normal and unusual behaviors or events to help mitigate potential threats. Gaps in awareness are a result of training and reinforcement, especially considering the makeup of the AOC workforce. Continuous training and reinforcement are key to improving the AOC's security posture.

Recent OIG work, including its 2025 report, White Paper on the Architect of the Capitol's Emergency Management (OIG-FLD-2025-02), and its 2021 report, Evaluation of the Architect of the Capitol's (AOC's) Emergency Preparedness Posture (2020-0002-IE-P), note that inconsistent sharing of threat assessment information across AOC offices and jurisdictions inhibits coordinated readiness. The AOC's internal processes for communicating emerging threats and security concerns are not fully standardized, and coordination efforts between the Capitol Police Board and U.S. Capitol Police (USCP) remain ongoing.

Emergency Preparedness

The AOC plays a key role in providing a safe environment across the Capitol campus, which hosts about 3 million visitors annually. As such, the AOC's emergency management and preparedness posture is a mission-critical function essential for protecting employees, the public, AOC property, and infrastructure.

The AOC continues to face elevated security challenges that place people, property, and historical resources at risk. Due to the high-visibility and accessibility of the Capitol campus, persistent threats that challenge readiness are incidents — including suspicious packages, disruptions affecting jurisdictions open to the public, and local security matters — that underscore the importance of clear, coordinated emergency response processes.

While the AOC has made progress improving its emergency management and preparedness posture, timely implementation should be prioritized. This includes providing staff with skills to meet the agency's safety responsibilities and remaining responsive to evolving emergency management challenges. Should implementation challenges persist, employee safety concerns may affect staff morale and well-being.

OIG's 2021 report, Evaluation of the Architect of the Capitol's (AOC's) Emergency Preparedness Posture (2020-0002-IE-P), found that the AOC's preparation and participation in multi-jurisdictional emergency management training was not always consistent; the AOC lacked a standardized emergency management training evaluation process; and AOC's organizational emergency action and response plans (EARPs) were not consistently updated or aligned with the AOC Base EARP in policy, structure, and guidance.

In FY 2025, OIG initiated a follow-up evaluation, Follow-up Evaluation of the Architect of the Capitol's Emergency Preparedness Posture (OIG-FLD-2026-01), to determine whether the AOC effectively implemented corrective actions to address the findings and recommendations in the OIG's 2021 evaluation report. While the report's distribution was limited due to the sensitive nature of the evaluation, OIG identified four findings and provided eight recommendations.

As the AOC's emergency preparedness posture continues to mature, the agency should consider implementing better oversight mechanisms and evaluating whether the current model provides the right people with the right skills to meet its safety mission and remain responsive to ongoing and evolving emergency management challenges.

Employment Suitability

Suitability evaluates the character, integrity, and conduct of potential employees, including contractors, to protect and promote the efficiency of AOC programs and operations. The United States Government Accountability Office's (GAO's) 2025 High Risk Series report identified the personnel security process involving adequate screening of employees handling sensitive information as a necessary step in preventing unauthorized disclosure.[3]

[3] GAO. (2025). High Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness, GAO-25-107743. https://files.gao.gov/reports/GAO-25-107743/index.html.

Although security badge access is managed by USCP for most Capitol complex entities, the AOC has a vital role in framing the security posture campus-wide by ensuring contractor documentation, vetting, and access procedures are complete, timely, and accurate. During FY 2026, the AOC issued a new suitability policy and made other enhancements to the program, responding, in part, to an OIG recommendation from July 2022.

OIG recognizes the critical importance of adequate suitability vetting for AOC staff and contractors and remains concerned about the suitability screening program despite these enhancements. OIG initiated a follow-up evaluation in July 2026 to determine whether the AOC's personnel and contractor suitability program is effectively designed and implemented to mitigate safety and security risks to the Capitol complex.

AGENCY PROGRESS



OIG recognizes several ongoing efforts to strengthen safety, security, suitability, and emergency preparedness.

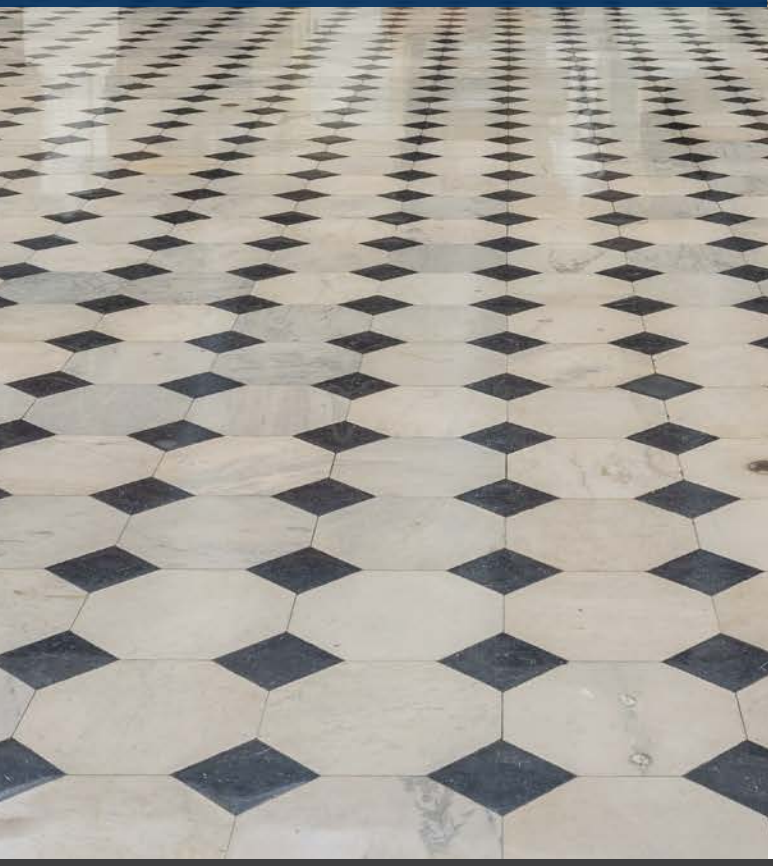
The agency has taken steps to address OIG recommendations regarding these matters, including hiring additional emergency management personnel. In addition, the AOC has approved policy mandating routine training initiatives. As previously indicated, the AOC also implemented a new suitability policy.

In addition, the AOC demonstrated a commitment to safety by pausing building construction/renewal in accordance with its contractual authority until safety requirements were met on the Cannon House Office Building Renewal Project. OIG's 2026 evaluation, Evaluation of the Cannon House Office Building Renewal (CHOBr) Project's Safety (OIG-AUD-2026-02), determined that the AOC's decision to suspend work and remediate potential issues was consistent with its contractual authority and appropriately aimed at ensuring the project site did not pose an immediate danger.

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 information technology (IT) services. Such disruptions could compromise data confidentiality, impede mission-critical functions, and affect the safety and security of the Capitol campus.

Since 2022, OIG has issued 3 reports and made 39 recommendations pertaining to information and cybersecurity. Of these, six recommendations remain open. Refer to the Information and Cybersecurity Risk Management section in Appendix A for a complete list of relevant reports.

KEY AREAS OF CONCERN

The AOC is responsible for the maintenance, development, and preservation of the Capitol campus and relies heavily on information systems containing highly sensitive information, including detailed Capitol complex designs, emergency preparedness documents, and operational procedures to support its responsibilities. These systems comprise multiple generations of technology, and management of antiquated and emerging technology in a cybersecurity-sensitive environment is a daily operations risk.

Key areas of concern include: (1) IT modernization, (2) expanded artificial intelligence (AI) use, and (3) supply chain risk.

Information Technology Modernization

Threats to information and cybersecurity are a continuous challenge in keeping AOC systems, employees, and other resources secure. To strengthen the AOC's cybersecurity posture, the Architect

identified, invested in, and implemented a Zero Trust Architecture (ZTA) program and associated toolset to raise AOC cybersecurity standards, reduce vulnerabilities, and limit potential impact of cyberattacks against the agency's systems and data. However, OIG work has identified opportunities for improvement, including its Evaluation of the Architect of the Capitol's Implementation of Information Security Modernization for Fiscal Year 2024 (2024-0004-IE-P). OIG initiated the review to determine whether the AOC developed and implemented effective information security programs and practices and provided the AOC with 12 findings and 16 recommendations.

Additionally, AOC submitted a budget request in FY25 to proactively replace IT hardware systematically before it becomes unsupported, insecure, unreliable, or incompatible with required software. However, due to budget constraints, this program has not been funded, and AOC jurisdictions have cited outdated technology as a long-standing source of operational and maintenance challenges. In some instances, outdated systems fail more frequently and become vulnerable to cybersecurity attacks, resulting in a decline in productivity that requires staff to resort to manual processes, introducing the risk of data inaccuracies, service disruptions, and potential mission execution risk.

Increases in intrusion attempts compounded by insufficient resources, limited staff capacity, and challenges keeping pace with evolving technology demands have increased the potential for network and service disruptions and exposure of security-sensitive information. As such, the AOC must make corresponding investments in innovative, proactive, and protective cybersecurity tools and techniques to better protect AOC users, data, and systems.

Given the mission-critical nature of AOC information systems and the evolving cybersecurity threat environment facing federal agencies, it is prudent for the AOC to continually assess whether relevant controls adequately mitigate operational and security risks.

To further support the AOC in navigating this topic, OIG recently initiated an evaluation of AOC's information security modernization and incident response that will be issued in FY 2027.

Timely investment in and implementation of information security practices and policies is necessary to secure critical systems, operations, and the identification of personnel. Failure to strengthen these areas could subject the organization to system vulnerabilities, such as unauthorized access and disclosure of information which can remain undetected for quite some time until discovered. These vulnerabilities can be minimized by enforcing policies, procedures, and practices that align with information system and cybersecurity best practices to the greatest extent possible.

Expanded Artificial Intelligence Use

The AOC's use of AI is expanding in ways that can offer important benefits to the agency. However, advances in AI also raise security considerations. AOC management has expressed concerns regarding the rapid development and increasing use of AI technologies and the evolving cybersecurity threats associated with those capabilities. The AOC must effectively and efficiently manage emerging technologies, such as AI and AI agents, to support employees using them to conduct official business for the agency. The AOC is challenged with ensuring employees only use AOC-approved AI tools in accordance with AOC policy and the availability of funding to meet program and operational needs.

Without strong governance and consistent oversight, AI poses an increased risk of producing unreliable outputs or undesirable results.

Supply Chain Risk

Recent OIG investigative activity indicates better controls are needed around system authorization and access, including policies and enforcement. AOC staff have also raised concerns that operational technology cybersecurity threats could put operations and infrastructure at risk — for example, bad actors could gain unauthorized access to critical infrastructure (e.g., boilers, chiller systems) and other building management control functions.

AOC operations and programs rely on the products and services provided by external vendors. While these products and services are often necessary to perform daily functions, utilizing these sources poses cybersecurity risk through the supply chain in which these products and services are procured. The AOC is faced with the challenge of establishing a governance program/structure for identifying and mitigating supply chain risk across offices and jurisdictions to identify red flags and prevent potential cybersecurity vulnerabilities introduced through third-party vendors and products.

In 2025, OIG issued its Evaluation of Architect of the Capitol's Supply Chain Risk Management (2024-0003-IE-P) and found that the AOC lacked a supply chain risk management governance program and that the risk management process for the AOC's offices and jurisdictions lacked consistency. OIG issued three recommendations, and the agency concurred with all.

AGENCY PROGRESS



The AOC has taken several steps to strengthen its information security controls and risk management practices.

In June 2026, the AOC issued Policy Memorandum 7-4 on AI, including authorized and prohibited uses, to amend the existing cybersecurity policy requirements. The AOC continues to expand its implementation of ZTA practices agencywide to ensure that only authorized users and devices can access critical resources. In response to raised security concerns, the AOC implemented stronger internal controls for contractors and employees and restricted access to certain systems and data. In addition to annual IT-policy compliance measures, all staff were required to sign an updated Rules of Behavior and Non-Disclosure Agreement in 2026.

The AOC is prioritizing the location of its data centers to bolster resiliency and continuity of operations to reduce exposure to physical and cyber-related threats. Further, the AOC's Office of the Chief Security Officer is in the process of hiring an Operational Technology Cybersecurity Specialist to develop policies and procedures around operational technology to strengthen cybersecurity controls and monitoring capabilities and address emerging threats and unauthorized access.

While these efforts demonstrate a commitment to strengthening the agency's cybersecurity posture, sustained investment in technology and cybersecurity 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 encompass 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.

Since 2022, OIG has issued 1 report, made 12 recommendations, processed numerous complaints, and completed several investigations pertaining to workforce management and accountability. No recommendations remain open. Refer to the Workforce Management and Accountability section in Appendix A for a complete list of relevant reports.

KEY AREAS OF CONCERN

Key areas of concern include: (1) recruitment and retainment of a highly skilled workforce and (2) employee misconduct and inconsistencies in accountability practices.

Concerns regarding human capital remain a high-risk area identified by GAO in 2025[3] and in previous years partly due to skills gaps, inefficient screening, and the inability to keep pace with staffing needs. While this area is no longer the AOC's highest-rated enterprise risk, the agency continues to experience shortages in critical skill areas.

Recruitment and Retention of a Highly Skilled Workforce

The AOC continues to face challenges recruiting and retaining a diverse, highly skilled workforce. AOC jurisdiction leadership has called attention to concerns regarding the limited availability of personnel with the technical expertise and trade-related skillsets necessary to sustain operations. The AOC views human capital

strategy, including the ability to attract, develop, and retain employees, as a key aspect of its strategic goal to foster an innovative and empowered workforce.

According to AOC staff, employee recruitment and retention is affecting many jurisdictions' ability to maintain critical operational capabilities. The AOC's salary ranges, particularly for highly specialized positions, are not competitive. These hiring difficulties have the potential to impact operations, institutional knowledge, and jurisdictions' ability to sustain essential infrastructure.

Recruitment depends on the AOC's ability to screen and onboard professional and trades staff while balancing complex — and sometimes lengthy — hiring processes. Succession planning, attributed to an aging workforce, and the need to enhance employee skills and sustain specialized trades are challenges for the agency.

A strong recruitment and retention strategy is essential to maintaining institutional knowledge and service quality. However, challenges remain, driven in part by resource limitations, which prevent implementation of identified training and workforce initiatives.

To strengthen the agency's human capital landscape, the AOC should continue to engage in regular evaluation of workforce strategies, succession planning, evolving skill requirements, compensation structures, and recruitment approaches to ensure the agency remains competitive.

In August 2024, OIG issued an evaluation, The Architect of the Capitol Human Capital Management Program Evaluation (2023-0003-IE-P), and found that the AOC had structured procedures for creating and disseminating AOC policy and that the Human Capital Management Division (HCMD) met five of seven key performance indicators. However, OIG also identified findings related to communication, operational inefficiencies, gaps in policy guidance and processes, and noncompliance with policy. OIG has since closed the 12 recommendations associated with that review.

Employee Misconduct and Inconsistencies in Accountability Practices

OIG continues to see a recurring trend in employee ethics and misconduct, including inconsistencies in managers' decisions to address misconduct at the administrative level and in leadership's ability to ensure penalties are fair across the board for similar policy violations.

Reported allegations of misconduct, including false medical documentation, time and attendance abuse, and theft, remain a problem. During the semiannual reporting period of October 1, 2025–March 31, 2026, OIG completed 5 investigations addressing ethical violations, misconduct, theft, and suspected fraud, and has since received 24 complaints of a similar nature. As the AOC strives to make the organization a better workplace, decisive, ethical leadership that implements consistent, corrective measures that hold employees accountable for misconduct at every level will continue to add value.

If inconsistent disciplinary actions continue to be an issue across AOC offices and jurisdictions, employees who report misconduct may lose trust in the process. Additionally, employees may feel that their concerns are not appropriately addressed following the adjudication of incidents. Low morale could become an issue when employees observe that disciplinary actions are different or contradict infractions addressed in AOC policy. AOC leadership should work to improve transparency in disciplinary actions, particularly when management decisions differ across offices and jurisdictions and may unintentionally give employees the perception of favoritism.

The AOC has already identified typical penalties for infractions; however, additional guidance regarding disciplinary decisions across the agency could add further support. AOC leadership has been proactive in addressing this issue, including engaging with HCMD and clarifying expectations with senior management.

AGENCY PROGRESS



The AOC's HCMD study on wage grade compensation to understand and address pay inequities and retention factors that impact skilled trade workers requires a definitive implementation timeline which has not yet been established. Although competitive salaries are essential, other factors are also 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.

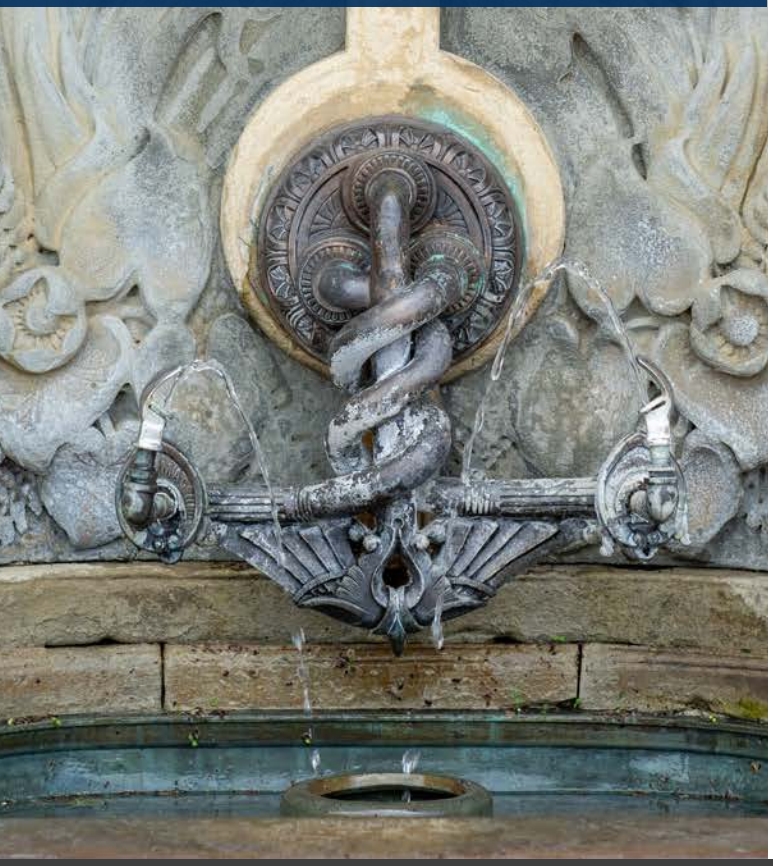
Additionally, although not formalized by policy, the AOC has taken initial steps and developed an internal disciplinary review board to provide comments on the consistency of disciplinary actions initiated across AOC offices and jurisdictions.

The AOC also has a training platform with resources available to ensure all employees adhere to AOC policies and general practices. Those resources include practical tools for management personnel to recognize and prevent fraud, waste, and abuse. The challenge exists in strengthening programs to further prevent such activities.

4. DATA GOVERNANCE, RECORDS RETENTION, AND PROCUREMENT

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. Management of procurement, the process by which the AOC acquires goods and services, relies on adequate data governance and records retention.

Since 2022, OIG has issued 29 reports, made 117 recommendations, and completed 1 investigation pertaining to data governance, records retention, and procurement. Of these, 22 recommendations remain open. Refer to the Data Governance, Records Retention, and Procurement section in Appendix A for a complete list of relevant reports.

KEY AREAS OF CONCERN

Key areas of concern include: (1) non-standardized documentation practices, (2) procurement, and (3) data quality.

Ongoing in most contract-related OIG work, data completeness and the ability to easily identify and locate files are recurring challenges. These potential internal control weaknesses impact OIG's oversight responsibilities designed to prevent and detect fraud, waste, and abuse. While some areas of concern have been addressed, the AOC continues to face challenges in applying uniform documentation procedures across jurisdictions. OIG requests sometimes yield delayed, incomplete, or missing records, prolonging oversight work. These conditions undermine transparency; limit data-driven insights into potential fraud, waste, abuse, and mismanagement; and elevate the agency's risk profile.

Enterprise-wide concerns persist regarding the AOC's ability to maintain reliable operational records, data integrity, and timely availability of information to make data-driven decisions.

Non-Standardized Documentation Practices

The AOC continues to face challenges ensuring employees adequately document and retain data and information, even after establishing a data management policy.[4] Documentation practices remain non-standardized and vary 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 2025 report, Audit of the Architect of the Capitol's Senate Furniture Program (OIG-AUD-2025-03), 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.

Procurement

Similar concerns arise in procurement documentation. OIG's 2026 report, Audit of the Architect of the Capitol's Unauthorized Commitments (OIG-AUD-2026-03), identified a lack of documentation to support unauthorized commitments (UACs) and ratifications. The AOC also lacks sufficient guidance and alternative solutions for transactions that meet the definition of a UAC despite not actually being accounted for as a UAC. The absence of sufficient guidance makes it difficult for AOC staff to determine how to prevent, identify, assess, and ratify a UAC. Additionally, OIG's 2026 report, Audit of Cannon House Office Building Renewal (CHOBr) Project's Contract Costs (OIG-AUD-2026-04), found that the contractor was unable to provide adequate documentation to support the validity of some invoiced costs. The AOC should ensure that it obtains sufficient supporting documentation that is readily available for examination.

Similarly, in its 2026 report, Follow-up Evaluation of the Architect of the Capitol's Information Technology Division Contracting Services Blanket Purchase Agreement (OIG-FLD-2026-02), OIG determined that the AOC does not have a documented process for reviewing and accepting independent government estimates (IGEs), and Contracting Officer's Representatives (CORs) were unaware of any guidance that required them to retain supporting documentation for IGEs in the COR contract files. AOC Order 34-1, Contracting Manual, does not specify documentation standards or expectations for how IGEs should be supported.

The inability to easily obtain complete data pertaining to AOC programs and contracts continues to be an ongoing issue across audits, evaluations, and investigations. While not a new challenge for the AOC, OIG work highlights the difficulty in accessing reliable and complete data to assess compliance and proper implementation of internal controls.

As these weaknesses persist, they demonstrate the need for documentation standards that support the lifecycle of AOC assets, policy revision, procedures, and automated or manual processes to improve procurement, data accuracy, and reporting capabilities across the AOC.

Beyond documentation-related issues, the AOC faces similar procurement challenges to other organizations, including potential fraud, waste, abuse, and mismanagement of appropriated funds and resources in procurement practices. In one recent investigation, OIG found that a small business vendor contracted to service the AOC's biological drain (bio-drain) pumps acted as a passthrough — an affiliate — to a larger business vendor in which the small business owner and sole employee provided

[4] AOC Policy 8-6 defines the roles and responsibilities of key data governance bodies as well as procedures and standards for effective data management, data security, and responsible data use.

the initial quote to the AOC and followed up on invoice payments, but the original large business continued to perform the work. While OIG did not find evidence of a personal relationship between the AOC employee/Contracting Officer and the contractors, OIG's investigation also found that similar contract work had been awarded in other AOC jurisdictions at a lower cost.

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.

OIG audit findings consistently indicate data quality challenges persist pertaining to documentation, the impact of which has led to overstated inventory costs, inaccurate records, insufficient documentation, the inability to locate assets, insufficient use of storage space, ineffective and redundant purchasing practices, and deficient safeguarding measures.

The AOC continues to rely on information systems comprising multiple generations of antiquated technology, limiting integration with new technologies and its ability to generate accurate, consolidated reporting and insights. Absent sufficient resources, the AOC will continue to experience fragmentation resulting in data silos, inefficiencies, and inconsistencies in how information is captured and used across the enterprise.

AGENCY PROGRESS



Although the AOC has taken steps to address previously identified deficiencies, adherence to policy and data management practices remains inconsistent across jurisdictions. Ensuring uniform application of existing standards will be critical to achieving sustained improvement. To support these issues in the procurement space, the AOC is revising its Contracting Manual and implemented numerous prior OIG recommendations related to procurement. Regarding data, the AOC has leveraged the work of a data governance board to align the use and management of data with agencywide goals and outcomes.

The agency further indicates that the Data Governance Council has established policies and guidance to promote enterprise-wide data quality, integrity, standardization, and consistency. These policies provide an overarching governance framework and establish expectations for how data should be managed, maintained, and reported across the AOC.

The AOC is also working to make data more accessible and increase data literacy across the workforce. The AOC's Office of the Chief of Operations reports developing multiple dashboards to improve operations, track performance, and gain insights to better understand how funds are utilized. 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.

The AOC's Records Management and Archives Branch indicates that between FY 2025 and FY 2026, it created or updated seven agency records schedules to support compliant, efficient recordkeeping. Efforts will continue in FY 2027.

5. CRITICAL INFRASTRUCTURE, DEFERRED MAINTENANCE, AND PRESERVATION MANAGEMENT

Status

NEW



Critical infrastructure, deferred maintenance, and preservation management refers to the AOC's ability to maintain and improve aging facilities, protect vital building systems and facilities, and preserve the heritage asset within AOC purview. Failures have the potential to disrupt congressional operations and compromise both safety and preservation elements of the AOC's mission.

Since 2022, OIG has issued two reports and made six recommendations pertaining to critical infrastructure, deferred maintenance, and preservation management. Of these, all six recommendations remain open. Refer to the Critical Infrastructure, Deferred Maintenance, and Preservation Management section in Appendix A for a complete list of relevant reports.

KEY AREAS OF CONCERN

Key areas of concern include: (1) critical infrastructure, (2) preservation management, and (3) deferred maintenance.

Capitol complex maintenance is both a priority and a challenge. An AOC FY 2025 Targeted Risk Assessment highlighted critical infrastructure failure as the agency's highest-rated risk. According to GAO,[5] the estimated cost of deferred maintenance and repair backlogs for federal agencies has more than doubled from $171 billion to $370 billion between FY 2017 and FY 2024. The AOC's budget request to address critical infrastructure needs underscores the effects of unfunded repair projects compounded in the form of deferred maintenance. The AOC's request rose 23 percent from $1.3 billion in FY 2026 to $1.6 billion for FY 2027.

[5] GAO. (2025). Testimony Before the House Subcommittee on Financial Services and General Government Committee on Appropriations: Federal Real Property: Disposing of Unneeded Facilities Could Help Reduce Maintenance Backlog. GAO-25-108400. https://www.gao.gov/assets/gao-25-108400.pdf.

Critical Infrastructure

The AOC's Capitol Complex Blueprint serves as a strategic framework for refurbishment, modernization, preservation, and sustainability initiatives across the complex. Within this plan, critical infrastructure repairs, enhanced security measures, and various other improvements are prioritized.

As CHOBr renovations wind down, planning for the Rayburn House Office Building (RHOB) renewal has begun. AOC indicates that a substantial portion of RHOB assets have exceeded their useful life expectancy — specifically, aging mechanical systems, persistent leaks, and structural issues that have made full-scale renewal essential. Within the last year, leaks disabled multiple congressional suites, and a fire impacted congressional operations. Accelerated deterioration due to aging infrastructure and insufficient funding results in increased maintenance costs and, in more extreme circumstances, needed repairs create the potential for unsafe workplace conditions.

Ongoing concerns pertain to the AOC's ability to deliver large-scale projects on schedule and within budget. Without a finalized strategic plan, transparency in operations becomes limited, potentially compromising the jurisdiction planning process. The House Appropriations Committee has also expressed concern regarding the "AOC's ability to deliver large-scale projects on schedule and within budget and to effectively implement the Capitol Complex Master Plan."[6]

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. Without adequate funding and a clear plan, the likelihood of accelerated deterioration, persistent delays, misdirected resources, and performance challenges increases.

Preservation Management

The AOC's mission to "serve, preserve, and inspire" requires construction, renewal, and maintenance activities to maintain the historic integrity of the Capitol campus while ensuring safe and functional operations. Preservation management risk is driven by age, complexity, and ongoing preservation and long-term infrastructure sustainability requirements. Adequate resources, including storage and archival expertise, are also required to prevent loss, deterioration, and mismanagement of these historic items.

Within the Library Buildings and Grounds Jurisdiction, pinhole failures have developed within sections of the sprinkler system piping within the Thomas Jefferson Building, resulting in water leaks and associated damage to the building infrastructure and priceless collections of books, maps, artifacts, and museum-related collections located within the building. It was noted that the sprinkler system replacement project was partially funded last year but not funded in FY 2026.

During FY 2026, OIG initiated an evaluation (2025-0001-IE-P) to determine the effectiveness and efficiency of the AOC's Historic Preservation and Stewardship Program, with an in-depth assessment of the AOC's management, maintenance documentation, and recordkeeping activities for heritage assets under its custodianship. The evaluation found that although the AOC's curation efforts have resulted in many positive accomplishments around databases, conservation, and education and outreach, there were opportunities to strengthen inventory management and recordkeeping of maintenance documentation for heritage assets. Specifically, OIG found issues regarding the completeness and accuracy of the listing of heritage assets and the associated maintenance documentation.

[6] H. Rept. 119-666 - Legislative Branch Appropriations Bill, 2027. (2026, September 30). https://www.congress.gov/committee-report/119th-congress/house-report/666/1.

Deferred Maintenance

Deferred maintenance refers to repair work on existing facilities and infrastructure that has not been performed on schedule or is delayed to a future period, resulting in full or partial asset failure and increasing the backlog[7] and risk. Such maintenance is associated with capital renewal of major infrastructure systems[8] and may result in the deterioration of an historic asset or the outright inability to use a facility as intended.

Within the last year, inconsistent funding has limited the AOC's ability to conduct critical maintenance; critical maintenance is most efficient when maintenance and repairs are performed as originally scheduled. Renovation and modernization efforts often involve significant uncertainty, as conditions and potentially hazardous materials (e.g., asbestos, lead-based paint) may not be fully known until construction activities begin. This has the potential to complicate project execution, increase costs, extend timelines, and create additional operational and budgetary pressures. Timely investment is essential to prevent system failures and mitigate safety concerns and disruption of congressional operations.

OIG recently initiated an evaluation of the AOC's Deferred Maintenance Management and Capital Renewal Program to assess the effectiveness of the AOC's planning, prioritization, and resource allocation for addressing deferred maintenance and capital renewal across Capitol complex facilities.

AGENCY PROGRESS

AOC leadership remains focused on deferred maintenance, critical infrastructure, and preservation management. In its FY 2025 Performance Accountability Report, the AOC recognized that "maintaining and modernizing the Capitol complex remains a central priority and our biggest challenge" and identified the Capitol complex master plan and enterprise asset management as ongoing strategic objectives.

The Enterprise Asset Management Program was established to address the backlog challenges and proactively identify future project requirements. Implementation is set to occur in phases.

OIG will conduct work on heritage asset management, deferred maintenance, and capital renewal in FY 2027 to further support agency progress in these areas.

[7] Backlog is defined as the total deferred maintenance plus capital renewal expected to be deferred maintenance within a 5-year window.
[8] Capital renewal is defined as the process of making replacements in kind, prior to failure, to correct unacceptable conditions caused by aged building components.

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.

KEY AREA OF CONCERN

The key area of concern is: (1) availability of protection, which includes 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.[9] Instead, protections originate within the Congressional Accountability Act,[10] which prohibits employing offices from intimidating, retaliating against, or discriminating against employees who report allegations of wrongdoing related to workforce rights covered by the act. The effectiveness of these protections depends on the AOC's internal procedures and the degree to which leadership fosters a culture that encourages reporting.

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.

[9] Public Law 101-12. Whistleblower Protection Act of 1989. https://uscode.house.gov/statviewer.html?volume=103&page=16.
[10] Public Law 104-1. Congressional Accountability Act of 1995. https://uscode.house.gov/statviewer.html?volume=109&page=3.

Though formal statutory whistleblower protections, including providing employees with protection from reprisal for reporting wrongdoing more broadly, would require legislative action, the AOC can take steps within its existing authority to strengthen its internal framework. Organizational culture is a key determinant in employees' willingness to report. Additional steps include devoting adequate resources to ensure effective systems are in place to protect reporters, inform them of their rights, and encourage timely responses. Other legislative branch agencies have implemented similar measures to strengthen reporting pathways and can serve as a model for enhancing AOC practices.

AGENCY PROGRESS



AOC has indicated that it has solicited information from other legislative branch agencies on best practices and that it intends to amplify internal policies pertaining to whistleblower activity. Additionally, the AOC recently hired two new ombuds to help non-bargaining employees navigate workplace concerns, questions, and conflicts.



Appendices



Appendix A



SUPPLEMENTAL INFORMATION

The following table lists reports relevant to each opportunity/challenge area.

1. Safety and Security

- Follow-up Evaluation of the Architect of the Capitol's Emergency Preparedness Posture (OIG-FLD-2026-01)
- White Paper on the Research of the Architect of the Capitol's (AOC'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)
- Evaluation of the Architect of the Capitol's (AOC's) Emergency Preparedness Posture (2020-0002-IE-P)
- Evaluation of the Cannon House Office Building Renewal (CHOBr) Project's Safety (OIG-AUD-2026-02)
- Flash Report Series – U.S. Capitol Building Window Installation, Preservation and Repair: Before and After January 6, 2021 (2022-0003-IE-P)

2. Information and Cybersecurity Risk Management

- Evaluation of Architect of the Capitol's Supply Chain Risk Management (2024-0003-IE-P)
- Evaluation of the Architect of the Capitol's Implementation of Information Security Modernization for Fiscal Year 2024 (2024-0004-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)

3. Workforce Management and Accountability

- The Architect of the Capitol Human Capital Management Program Evaluation (2023-0003-IE-P)
- Identity Theft (2025-0014-INVI-P)
- Time and Attendance Abuse Allegations (2025-0017-INVI-P)
- Time and Attendance Fraud (2025-0015-INVI-P)
- Consumption of Alcohol While on Duty (2026-0002-INVI-P)
- Contracting Violations (2025-0006-INVI-P)
- Misuse of Government-Issued Mobile Device for Inappropriate Communications (2025-0009-INVI-P)
- Overtime Abuse (2024-0013-INVI-P)
- Time and Attendance Fraud (2024-0023-INVI-P)
- Fraudulent Medical Documentation (2025-0011-INVI-P)
- Clear, Consistent, and Uniform Application of Architect of the Capitol (AOC) Policy (2023-0006-INVM-P)
- 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)

4. Data Governance, Records Retention, and Procurement

- Audit of the Architect of the Capitol's Unauthorized Commitments (OIG-AUD-2026-03)
- Audit of Cannon House Office Building Renewal (CHOBr) Project's Contract Costs (OIG-AUD-2026-04)
- Evaluation of Architect of the Capitol's Historic Preservation and Heritage Asset Management (2025-0001-IE-P)
- Follow-up Evaluation of the Architect of the Capitol's Information Technology Division Contracting Services Blanket Purchase Agreement (OIG-FLD-2026-02)
- Contracting Violations (2025-0006-INVI-P)
- Audit of the Cannon House Office Building Renewal Project's Substantial & Final Completion for Phase 3 & Phase 4 (OIG-AUD-2025-02)
- 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)
- Audit of Fiscal Year 2024 Financial Statements (OIG-AUD-2025-01)
- Audit of Fiscal Year 2025 Financial Statements (OIG-AUD-2026-01)
- Audit of Architect of the Capitol's Cannon House Office Building Renewal Project's Contract Labor (OIG-AUD-2025-04)
- Audit of the Architect of the Capitol's Construction Division (OIG-AUD-2024-06)
- Evaluation of Architect of the Capitol's Contracting Officer and Contracting Officer's Representative Oversight (2023-0002-IE-P)
- Follow-Up Evaluation of the Architect of the Capitol Data Center (OIG-FLD-2024-01)
- Fiscal Year 2023 Financial Statements Audit Management Letter (OIG-AUD-2024-02)
- Cannon House Office Building Renewal Project's Punch List And Warranty Work Process Lacked Sufficient Oversight (OIG-AUD-2023-08)
- Semiannual Review of the Architect of the Capitol's (AOC's) Multimillion-Dollar Construction Project Change Orders (OIG-AUD-2023-07)
- The Architect of the Capitol Lacked Sufficient Oversight of the Cannon Caucus Room Renovations (OIG-AUD-2023-06)
- Follow-Up Evaluation of the Architect of the Capitol's Inventory Accountability and Controls (OIG-FLD-2023-01)
- Flash Report Series – Architect of the Capitol's Records and Archives Management (2023-0001-IE-P)
- Architect of the Capitol's (AOC's) Internal Control Plan Lacked Procedures to Assess and Monitor Payment Accuracy (OIG-AUD-2023-05)
- Review of the Architect of the Capitol's (AOC's) Multimillion-Dollar Construction Project Change Orders (OIG-AUD-2023-04)
- Fiscal Year 2022 Financial Statements Audit Management Letter (OIG-AUD-2023-02)
- Audit of Fiscal Year 2022 Financial Statements (OIG-AUD-2023-01)
- Multi-Million-Dollar Construction Projects' Contract Provisions Comply with Federal Guidance, AOC Policies and Industry Standards Although Improvements Can Be Added (OIG-AUD-2022-07)
- Evaluation of the Information Technology Division's Inventory Accountability and Controls (2022-0002-IE-P)
- Audit of Fiscal Year 2021 Financial Statements (OIG-AUD-2022-04)
- Fiscal Year 2021 Financial Statements Audit Management Letter (OIG-AUD-2022-05)
- Architect of the Capitol Repetitively Reimbursed Small-Dollar Amounts of Unallowable Costs to the Contractor on the Cannon House Office Building Renewal Project (OIG-AUD-2022-01)

5. Critical Infrastructure, Deferred Maintenance, and Preservation Management

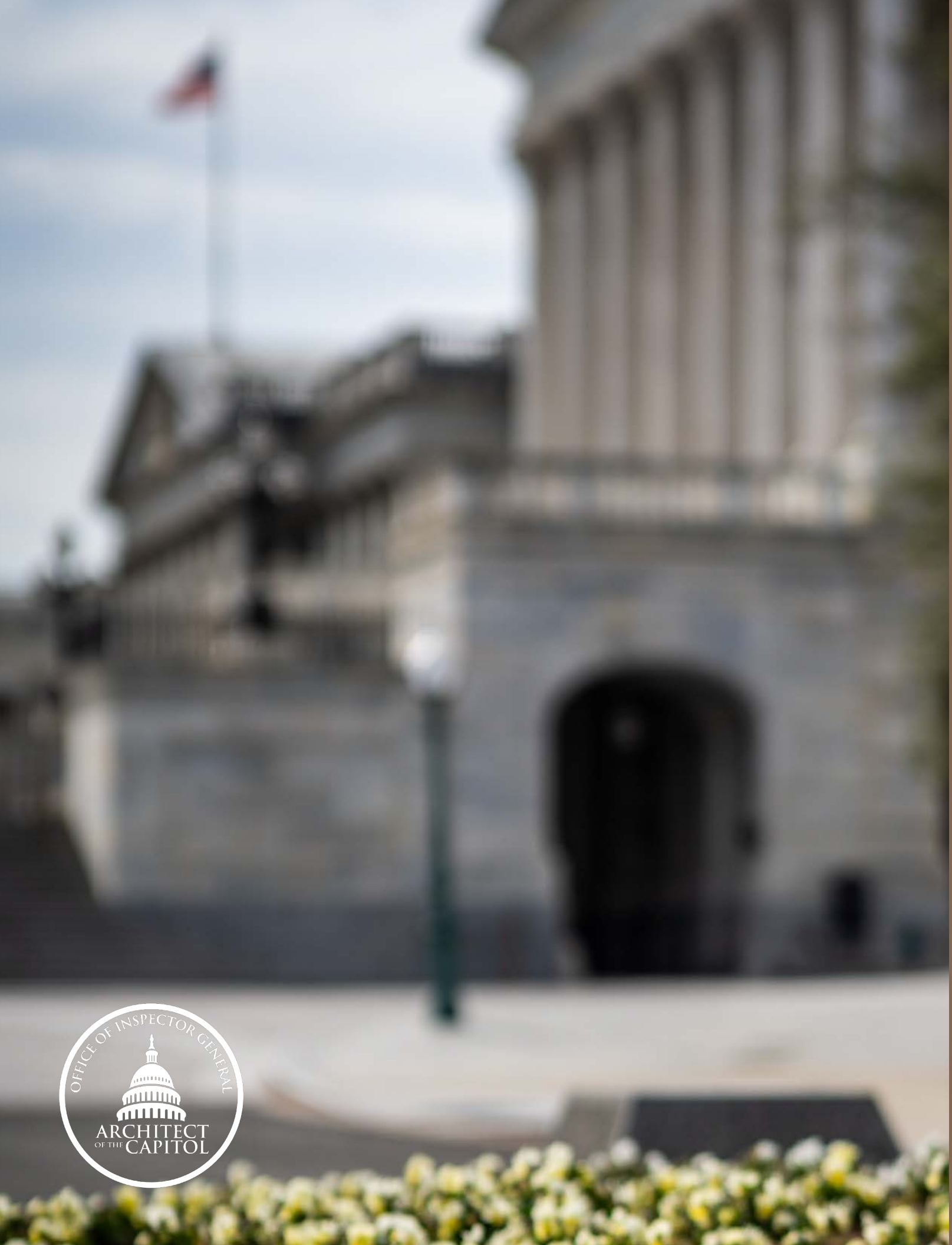
- White Paper on the Research of the Architect of the Capitol's (AOC's) Management of Deferred Maintenance and Capital Renewals (OIG-AUD-2024-04)
- Evaluation of Architect of the Capitol's Historic Preservation and Heritage Asset Management (2025-0001-IE-P)

Appendix B



LIST OF ACRONYMS USED

Term	Definition
AI	artificial intelligence
AOC	Architect of the Capitol
CHOBr	Cannon House Office Building Renewal
COR	Contracting Officer's Representative
EARP	emergency action and response plan
FY	fiscal year
GAO	United States Government Accountability Office
HCMD	Human Capital Management Division
IGE	independent government estimate
IT	information technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
RHOB	Rayburn House Office Building
UAC	unauthorized commitment
USCP	U.S. Capitol Police
ZTA	Zero Trust Architecture


OFFICE OF INSPECTOR GENERAL
ARCHITECT OF THE CAPITOL