INSPECTOR GENERAL

May 9, 2024

Follow-Up Evaluation of the Architect of the Capitol Data Center

Report No. OIG-FLD-2024-01

FINAL REPORT

MISSION

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

VISION

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

Results in Brief

Follow-Up Evaluation of the Architect of the Capitol Data Center

May 9, 2024

Objective

Our objective was to determine whether the Architect of the Capitol (AOC) effectively implemented corrective actions to address the findings and recommendations in the September 2019 Office of Inspector General (OIG) report, Audit of the AOC Data Center (OIG-AUD-2019-04). The September 2019 OIG audit found that the AOC's Information Technology Division (ITD) lacked sufficient controls over physical access to the AOC Data Center in the offsite facility (OSF).

In addition, during the September 2019 audit, the OSF experienced a power outage that impacted all tenants in the OSF. The OIG observed that a structured process was not in place for OSF tenants to properly communicate and coordinate with the Facility Management.

This evaluation followed up on the one finding and the two recommendations made to address improvements to physical access controls and the AOC's efforts to enhance communication and coordination with OSF tenants to mitigate the risk of unplanned power outage and maintain critical operations.

Findings

Based on our follow-up evaluation, we found that the AOC implemented the OIG's recommendations in the September 2019 OIG audit report by complying with updated procedures for requesting Data Center access for non-ITD personnel. However, we found that the AOC did not comply with procedures to monitor AOC Data Center access. Specifically, ITD did not comply with its standard operating procedure (SOP) that required them to create and maintain an ITD Authorized Access List for proxy card access and conduct annual validation and quarterly reconciliation of access to the AOC Data Center in the OSF.

Findings (Cont'd)

In addition, we observed that the AOC enhanced its communication and coordination efforts for OSF tenants by providing monthly updates to stakeholders and publishing emergency communication procedures.

Recommendations

We recommend that:

1. The AOC Chief Information Officer (CIO) require ITD to create and maintain an ITD Authorized Access List, in accordance with the ITD Authorized Data Center Proxy Card Access List Maintenance SOP.

2. The CIO require ITD to perform an annual validation of the ITD Authorized Access List, in accordance with ITD Authorized Data Center Proxy Card Access List Maintenance SOP.

3. The CIO require ITD to reconcile the ITD Authorized Access List against the United States Capitol Police Access Clearance Definition Report, at the end of every calendar quarter in accordance with ITD Authorized Data Center Proxy Card Access List Maintenance SOP.

Management Comments

The AOC provided comments on April 19, 2024, see Appendix C. In its Management Comments, the AOC concurred with all three recommendations. Please see the Recommendations Table on the following page for the status of the recommendations.

Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
CIO		1, 2, 3	

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

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

INSPECTOR GENERAL

DATE: May 9, 2024

TO: Joseph DiPietro, PE
Acting Architect of the Capitol

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

SUBJECT: Follow-Up Evaluation of the Architect of the Capitol (AOC) Data Center (Report No. OIG-FLD-2024-01)

Please see the attached final report for our follow-up evaluation of the Architect of the Capitol (AOC) Data Center, which we announced on September 12, 2023. Based on our follow-up evaluation we found that the AOC implemented the Office of Inspector General's (OIG's) recommendations in the September 2019 OIG report, Audit of the AOC Data Center (OIG-AUD-2019-04), by complying with updated procedures for requesting Data Center access for non-Information Technology Division personnel. However, we found that the AOC did not comply with standard operating procedures to monitor AOC Data Center access. We made three recommendations to improve monitoring of AOC's Data Center access.

In your response to our official draft report (see Appendix C), you concurred with all three recommendations. Based on your responses to Recommendations 1 through 3, we feel the proposed corrective actions address our recommendations. The status of the recommendations will remain open until final corrective action is taken. We will contact you within 90 days to follow up on the progress of your proposed management decisions.

We appreciate the courtesies extended to the staff during the evaluation. Please direct questions to Brittany Banks, Assistant Inspector General for Follow-Up at Brittany.Banks@aoc.gov or 202.436.1445.

Distribution List:

Angela Freeman, General Counsel
Telora Dean, Chief Administrative Officer
Aaron D. Altwies, Chief Security Officer
Robert Bell, Chief Information Officer
Darius Maddox, Chief Information Security Officer
Hajira Shariff, AOC Liaison to the OIG

CONTENTS

INTRODUCTION

Objective

The objective of this follow-up evaluation was to determine whether the Architect of the Capitol (AOC) effectively implemented corrective actions to address the findings and recommendations in the September 2019 Office of Inspector General (OIG) report, Audit of the AOC Data Center (OIG-AUD-2019-04).

Background

2019 OIG Audit Report

In August 2018, the AOC OIG initiated an audit of the AOC Data Center in the Offsite Facility (OSF) (formally known as the Alternate Computer Facility). The September 2019 OIG report, Audit of the Architect of the Capitol Data Center, focused on the review of policies and procedures to protect the physical integrity of the AOC Data Center and the information resource systems residing within. Specifically, the audit evaluated the AOC Data Center's access controls, environmental factors and back-up procedures designed to ensure the continuity of AOC information technology operations.

The 2019 OIG audit report found that AOC's Information Technology Division (ITD) lacked sufficient controls over physical access to the AOC Data Center in the OSF. The OIG found no issues with the approvals and access granted but determined that ITD's process for reviewing and reconciling access for non-ITD personnel was not sufficient. The ITD Proxy Access Card Standard Operating Procedures (SOPs), only specified control procedures for ITD personnel access to the AOC Data Centers.

During the audit, the OSF experienced a power outage that impacted all tenants in the facility. A lightning arrestor failure within the primary switchgear supporting the OSF caused the outage. All Data Centers operated on batteries for 60 minutes until the batteries were drained and remained off-line until commercial power was restored. The AOC noted in the outage incident report that the lack of communication and notification SOPs prevented Facility Management from responding quickly to the outage.

Additionally, the OIG found that OSF Facility Management did not regularly inform ITD of operational status performance measures and indicators, and that OSF tenants had significant concerns regarding inadequate communication for facility maintenance and repair operations. Facility Management stated that communication and coordination with OSF tenants was enhanced after the power outage by providing monthly operational status updates and publishing emergency communication procedures. The OIG advised the AOC to continue efforts to mitigate the risk of unplanned power outages and maintain critical operations.

This evaluation follows up on the two recommendations made to address improvements to physical access controls and the AOC's efforts to enhance communication and

coordination with OSF tenants to mitigate the risk of unplanned power outage and maintain critical operations.

AOC Data Center in the Offsite Facility

The OSF provides redundant components for the critical power infrastructure, and a single, non-redundant distribution path for serving the physical environment and temperature control for Data Center operations for multiple legislative branch agencies. The legislative branch agencies include the U.S. House of Representatives, the U.S. Senate, the Library of Congress, the United States Capitol Police (USCP), the Government Accountability Office (GAO), the Government Publishing Office, the Congressional Budget Office and the AOC.

AOC's Office of the Chief Security Officer

The AOC's Office of the Chief Security Officer (OCSO), also referred to as "Facility Management," is responsible for facility management and tenant services, including building maintenance, custodial services, Data Center infrastructure management, capital renewal, as well as facility renovation, modification and construction at the OSF.

AOC's Information Technology Division

ITD is the primary operational information technology (IT) organization supporting the AOC Chief Information Officer (CIO). The ITD is responsible for the design, development, maintenance, enhancement, and operation of the AOC's automated information systems, including AOC Data Center operations. The CIO is authorized to grant, suspend, revoke, or modify access to IT systems under the AOC's control. The ITD Proxy Card Access Manager is responsible for managing access to the AOC Data Center.

Criteria

- AOC Order 7-4, Information Technology Security, October 10, 2017
- AOC Order 8-2, Information Technology Management, March 22, 2019
- CIO Memorandum "Improving physical access controls to the AOC Data Center at the ACF," September 3, 2019
- SOP "ITD Authorized Data Center Proxy Card Access List Maintenance," September 3, 2019
- GAO-14-704G, Standards for Internal Control in the Federal Government (the Green Book), September 10, 2014 (Referenced as a best practice)

Finding

The AOC Did Not Comply with Procedures to Monitor AOC Data Center Access

In the 2019 report, the OIG found that the ITD lacked sufficient controls over physical access to the AOC Data Center in the OSF. The OIG identified 25 non-ITD personnel that accessed the AOC Data Center in the OSF from October 1, 2017, through September 30, 2019. The OIG found no issues with the approvals and access granted for ITD personnel, but determined that ITD's process for approving, reviewing and reconciling access for non-ITD personnel was not sufficient. For example, USCP approved 25 non-ITD personnel that ITD did not track. ITD acknowledged that they had no control over approval of non-ITD personnel access to the AOC Data Center. The OIG found that the ITD Proxy Access Card Standard Operating Procedures, dated January 29, 2015, only specified control procedures for ITD personnel access to the AOC Data Centers. The OIG concluded without proper physical access controls for the AOC Data Center in the OSF, ITD's sensitive network computer equipment and technology may be at risk for unauthorized access, theft, or tampering. The audit made two recommendations to address improvements to physical access controls.

Previous Recommendations

- We recommend that the Chief Information Officer review and revise its Standard Operating Procedures, *ITD Authorized Data Center Proxy Card Access List Maintenance* to account for non-ITD personnel.

- We recommend that the Chief Information Officer enhance its communication and coordination with USCP and other AOC jurisdictions to improve physical access controls to the Data Center at the OSF for non-ITD personnel.

Evaluation Results

Updates to Managing AOC Data Center Physical Access

AOC concurred with the recommendations of the 2019 OIG audit report. In response to Recommendation 1, the AOC revised its ITD Authorized Data Center Proxy Card Access List Maintenance SOP to include access control procedures for non-ITD personnel. In response to Recommendation 2, the CIO submitted a memorandum to the OCSO and the USCP on September 3, 2019, establishing a revised process to improve physical access controls for non-ITD personnel. The memorandum stated any requests to USCP for

access to the AOC Data Center shall come only from the designated ITD Proxy Card Access Manager or the AOC CISO.

Additionally, ITD Authorized Data Center Proxy Card Access List Maintenance SOP now requires ITD approval for all personnel, except for those needed for USCP essential functions. Based on our review of access requests, ITD complied with its updated procedures for requesting access for non-ITD personnel. We reviewed the Access Clearance Definition Reports (ACDRs) from October 1, 2019, through September 30, 2023. We identified that 81 personnel had access to the AOC Data Center. Out of the 81 personnel, the USCP provided nine non-ITD personnel with access to the AOC Data Center during our review period. We reviewed the USCP Security Access Control Forms for the nine non-ITD personnel and determined that ITD requested their access in accordance with the updated SOP and CIO memorandum.

Annual Validation of the ITD Authorized Access List

Our follow-up evaluation found that ITD did not comply with its SOP that requires them to create and maintain an ITD Authorized Access List for proxy card access to the AOC Data Center in the OSF. According to the SOP, this list should contain the names of personnel who are authorized to access the AOC Data Center. The SOP also requires ITD to conduct annual validations and quarterly reconciliations of access to the AOC Data Center.

As of the cutoff date of this report, ITD relies on the reports from USCP to validate AOC Data Center access. The ITD Proxy Card Access Manager coordinates with ITD staff to request proxy card access for individuals from USCP. USCP processes the requests and provides ITD with an ACDR on a quarterly basis. The ITD Proxy Card Access Manager sends the ACDR to ITD supervisors to validate access. The ITD stated there was no need to maintain their own list because the ACDR generated from the USCP access system contains the most accurate personnel access records.

Referenced as a best practice, GAO's Standards of Internal Control in the Federal Government (also known as the Green Book[1]), Principle 16 states that management should perform ongoing monitoring of the design and operating effectiveness of the internal control system as part of the normal course of operations. Ongoing monitoring includes regular management and supervisory activities, comparisons, reconciliations, and other routine actions. Without the implementation of existing internal controls, there is an increased risk of unauthorized personnel gaining access to AOC's sensitive and mission-essential information technology. To reduce the risk of unauthorized access, ITD should create an ITD Authorized Access List and adhere to existing internal controls (procedures) for monitoring physical access to the AOC Data Center.

[1] While the Legislative Branch is not required to abide by the standards set forth in the Green Book under the Federal Managers' Financial Integrity Act, these standards are best practice and an applicable framework for setting and vetting internal controls.

Quarterly Reconciliation of the ITD Authorized Access List

We found that ITD did not comply with its SOP which requires them to reconcile the ACDR and ITD Authorized Access List every quarter to ensure agreement and take necessary actions to add or remove user access. USCP relies on emails from the ITD Proxy Card Access Manager or the House Badging Office to grant, update, or revoke access. USCP staff manually enter information into their system which generates the ACDR. USCP stated that they do not review or validate any information in the system. They believe that it is the sole responsibility of the AOC to inform them of any changes to access. To reduce the risk of unauthorized personnel retaining unrestricted access to mission-critical AOC systems and data, ITD should follow established procedures to reconcile the ACDR and ITD Authorized Access List to account for all personnel with AOC Data Center access.

Recommendations

Recommendation 1

We recommend that the Chief Information Officer require the Information Technology Division (ITD) to create and maintain an ITD Authorized Access List, in accordance with the ITD Authorized Data Center Proxy Card Access List Maintenance standard operating procedure.

Recommendation 1 – AOC Comment

Concur. Based on the OIG's draft report (March 28, 2024), ITD has created the ITD Authorized Access List as a baseline in April 2024 and will maintain it in accordance with the ITD Authorized Data Center Proxy Card Access List Maintenance standard operating procedure (SOP). The SOP requires ITD to save the requesting and notifying emails for access changes, which ITD can provide as evidence along with the ITD Authorized Access List in August 2024 to close the recommendation.

Recommendation 1 – OIG Comment

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

Recommendation 2

We recommend that the Chief Information Officer require the Information Technology Division (ITD) to perform an annual validation of the ITD Authorized Access List, in accordance with ITD Authorized Data Center Proxy Card Access List Maintenance standard operating procedure.

Recommendation 2 – AOC Comment

Concur. Since the OIG's original report in September 2019 (OIG-AUD-2019-04), ITD has performed and will continue to perform regular reviews and validations of the USCP Access Clearance Definition Reports. ITD has modified this review process to more strictly comply with the ITD Authorized Data Center Proxy Card Access List Maintenance SOP. In cooperation with the USCP, ITD established its baseline in April 2024 of the ITD Authorized Access List and will continue to validate it at least annually in accordance with the ITD Authorized Data Center Proxy Card Access List Maintenance SOP. The SOP requires the ITD Proxy Card Access List Manager to email ITD supervisors as well as applicable AOC supervisors, or their designated contacts, or non-ITD staff on the Authorized Access List to confirm their continuation of access. The next validation will be completed by April 2025 and ITD can provide the requesting email and supervisory replies as evidence of validation no later than May 2025.

Recommendation 2 – OIG Comment

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

Recommendation 3

We recommend that the Chief Information Officer require the Information Technology Division (ITD) to reconcile the ITD Authorized Access List against the United States Capitol Police Access Clearance Definition Report, at the end of every calendar quarter in accordance with ITD Authorized Data Center Proxy Card Access List Maintenance standard operating procedure.

Recommendation 3 – AOC Comment

Concur. ITD is currently reconciling the ITD Authorized Access List against the USCP Access Clearance Definition Report and will continue to do so quarterly in accordance with the ITD Authorized Data Center Proxy Card Access List Maintenance SOP. After April 2024, USCP agreed to provide their next quarterly reports in August (for the 4th quarter) and December (for the 1st quarter of Fiscal Year 2025), which ITD can provide as evidence along with ITD's Authorized Access Lists and any reconciliation required in January 2025 as evidence of reconciliation.

Recommendation 3 – OIG Comment

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

Observation

The AOC Enhanced Its Communication and Coordination Efforts for OSF Tenants

In 2018, the OSF experienced a power outage that impacted all tenants in the OSF. The facility did not automatically switch to generator power for the critical systems and the generators did not automatically power the uninterrupted power supply systems as designed. The generators were manually started but were not able to connect to Data Centers' loads due to damaged electronic systems. All Data Centers operated off batteries for 60 minutes until they were drained and remained off-line until commercial power was restored. Per the Incident Summary Report, Facility Management noted that Facility Management did not have sufficient communication and notification SOPs in place to quickly respond to outage incidents.

The 2019 OIG report found that a structured process was not in place for OSF tenants to properly communicate and coordinate with the Facility Management. The OIG report stated, per ITD officials, Facility Management did not regularly inform ITD of operational status performance measures and indicators. The Facility Management also acknowledged that inadequate communication with CIOs and stakeholders regarding facility maintenance and repair operations were reported as major tenant concerns.

During the audit, Facility Management stated that communication and coordination with OSF tenants was enhanced post power outage by providing monthly operational status updates to OSF tenants and publishing emergency communication procedures. The OIG stated AOC should continue efforts to mitigate the risk of unplanned power outages and maintain critical operations.

Our follow-up evaluation found that Facility Management enhanced its process for communicating and coordinating with OSF tenants, which the OIG noted as an observation during the 2019 OIG audit. We observed that:

- Facility Management held monthly briefings with OSF tenants and bimonthly briefings with Data Center CIOs to provide information on facility updates, facility maintenance, operational status dashboards, upcoming activities, project status and facility performance measures.

- In July 2019, Facility Management created a Memorandum of Understanding (MOU) between the AOC and legislative branch agencies operating at the OSF. The purpose of the MOU was to define the terms and conditions for occupying and conducting business operations. The MOU outlined communication strategies that should be used for both normal business operations and emergencies. Since the MOU was drafted, it has undergone multiple revisions and is not yet final.

- Facility Management created an OSF Incident Communication Plan, which provides actions required to establish and maintain communications in the event of an incident impacting the mission of the OSF. The plan details a notification hierarchy to ensure Facility Management notifies appropriate personnel when an incident occurs.

- Facility Management created an "AOC Communications to OSF Stakeholders" document that describes who OSF stakeholders should contact when they identify routine or outage issues at the OSF.

APPENDIX A

Scope and Methodology

We conducted this evaluation from September 2023 through January 2024 in accordance with the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Inspection and Evaluation (also known as the Blue Book).[2] These standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our evaluation objectives.

This follow-up evaluation was self-initiated by the AOC OIG and was included in our FY 2024 Work Plan. The objective of this follow-up evaluation was to determine whether the AOC effectively implemented corrective actions to address the findings and recommendations in the September 2019 OIG report, Audit of the AOC Data Center (OIG-AUD-2019-04).

To address our evaluation objective, we reviewed relevant AOC policies and procedures, interviewed AOC and USCP staff, and followed up on the implementation of prior AOC results and recommendations.

Use of Computer-Processed Data

We used computer-processed data to perform a part of this evaluation. The computer processed data included nine ACDRs from October 1, 2019, through September 30, 2023, provided by ITD, to determine if ITD complied with its updated procedures for requesting access for non-ITD personnel to the AOC Data Center in the OSF. The ACDRs were extracted from the USCP access system. To assess how non-ITD personnel were granted access, we reviewed source documentation (Security Access Control Forms). Based on our understanding of the USCP system and the review of Security Access Control Forms, we can conclude that the computer processed data in the ACDRs is sufficiently reliable for the purpose of our follow-up evaluation.

Prior Coverage

Prior OIG report relevant to this follow-up evaluation include Audit of the AOC Data Center (OIG-AUD-2019-04).

[2] CIGIE. 2020. Quality Standards for Inspection and Evaluation (Blue Book). https://www.ignet.gov/sites/default/files/files/QualityStandardsforInspectionandEvaluation-2020.pdf

APPENDIX B

Notification Letter

ARCHITECT OF THE CAPITOL

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

www.aoc.gov

United States Government

MEMORANDUM

DATE: September 12, 2023

TO: Chere Rexroat, RA
Acting Architect of the Capitol

FROM: Christopher P. Failla, CIG
Inspector General

SUBJECT: Announcement for Follow-up Evaluation of the Architect of the Capitol (AOC) Data Center (2023-0002-FLD-P)

This is to notify you that the Office of Inspector General (OIG) is initiating a follow-up evaluation of the September 2019 OIG report, Audit of the Architect of the Capitol (AOC) Data Center, (OIG-AUD-2019-04). Our objective is to determine whether the AOC has effectively implemented corrective actions to address the findings and recommendations in the September 2019 OIG report.

Please provide an agency point of contact for this follow-up evaluation. We will contact the appropriate AOC offices to schedule an entrance conference in the upcoming weeks. If you have any questions, please contact Brittany Banks, Assistant Inspector General for Follow-Up, at 202.436.1445 or Brittany.Banks@aoc.gov.

Distribution List:

Joseph DiPietro, Acting Assistant to the Architect & Chief of Operations
Hajira Shariff, IG Liaison
Angela Freeman, Acting General Counsel
Teresa Bailey, POC for Chief Administrative Officer
Robert Bell, Chief Information Officer
Valerie Hasberry, Chief Security Officer

APPENDIX C

Management Comments

ARCHITECT OF THE CAPITOL

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

www.aoc.gov

United States Government

MEMORANDUM

DATE: April 19, 2024

TO: Christopher P. Failla
Inspector General

FROM: Joseph R. DiPietro, PE
Acting Architect of the Capitol

SUBJECT: Management Response to the Follow-Up Evaluation of the Architect of the Capitol Data Center (Project No. 2023-0002-FLD-P)

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) official draft of the subject report. The Architect of the Capitol (AOC) provides the following management response:

Recommendation 1
We recommend that the Chief Information Officer require the Information Technology Division (ITD) to create and maintain an ITD Authorized Access List, in accordance with the ITD Authorized Data Center Proxy Card Access List Maintenance standard operating procedure.

AOC Response
The AOC concurs with the recommendation. Based on the OIG's draft report (March 28, 2024), ITD has created the ITD Authorized Access List as a baseline in April 2024, and will maintain it in accordance with the ITD Authorized Data Center Proxy Card Access List Maintenance standard operating procedure (SOP). The SOP requires ITD save the requesting and notifying emails for access changes, which ITD can provide as evidence along with the ITD Authorized Access List in August 2024 to close the recommendation.

Recommendation 2
We recommend that the Chief Information Officer require the Information Technology Division (ITD) to perform an annual validation of the ITD Authorized Access List, in accordance with ITD Authorized Data Center Proxy Card Access List Maintenance standard operating procedure.

AOC Response
The AOC concurs with the recommendation. Since the OIG's original report in September 2019 (OIG-AUD-2019-04), ITD has performed and will continue to perform regular reviews and validations of the United States Capitol Police (USCP) Access Clearance Definition Reports. ITD has modified this review process to more strictly comply with the ITD Authorized Data Center Proxy Card Access List Maintenance standard operating procedure. In cooperation with

APPENDIX C

Management Comments

the USCP, ITD established its baseline in April 2024 of the ITD Authorized Access List and will continue to validate it at least annually in accordance with the ITD Authorized Data Center Proxy Card Access List Maintenance standard operating procedure. The SOP requires the ITD Proxy Card Access Manager to email ITD supervisors as well as applicable AOC supervisors, or their designated contacts, of non-ITD staff on the Authorized Access List to confirm their continuation of access. The next validation will be completed by April 2025 and ITD can provide the requesting email and supervisor replies as evidence of validation no later than May 2025.

Recommendation 3
We recommend that the Chief Information Officer require the Information Technology Division (ITD) to reconcile the ITD Authorized Access List against the United States Capitol Police Access Clearance Definition Report, at the end of every calendar quarter in accordance with ITD Authorized Data Center Proxy Card Access List Maintenance standard operating procedure.

AOC Response
The AOC concurs with the recommendation. ITD is currently reconciling the ITD Authorized Access List against the USCP Access Clearance Definition Report and will continue to do so quarterly in accordance with the ITD Authorized Data Center Proxy Card Access List Maintenance standard operating procedure. After April 2024, USCP has agreed to provide their next quarterly reports in August (for Q4) and December (for Q1 FY2025) which ITD can provide as evidence along with ITD's Authorized Access Lists and any reconciliation required in January 2025 as evidence of reconciliation.

Doc. No. 240402-02-01

ACRONYMS AND ABBREVIATIONS

ACDR	Access Clearance Definition Report
AOC	Architect of the Capitol
CIO	Chief Information Officer
GAO	Government Accountability Office
IT	Information Technology
ITD	Information Technology Division
MOU	Memorandum of Understanding
OCSO	Office of the Chief Security Officer
OIG	Office of Inspector General
OSF	Offsite Facility
SOP	Standard Operating Procedure
USCP	United States Capitol Police

INSPECTOR GENERAL
499 S. CAPITOL ST, SW
SUITE 518
WASHINGTON, DC 20515
www.aoc.gov