



# INSPECTOR GENERAL

SEPTEMBER 27, 2019

## **AUDIT OF THE ARCHITECT OF THE CAPITOL DATA CENTER**

*Report No. OIG-AUD-2019-04* **Redacted**

*Specific information about the Architect of the Capitol's Data Centers  
have been redacted from the publicly released version of this 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.



September 27, 2019

## Objective

To determine whether the Architect of the Capitol (AOC) developed and implemented policies and procedures to protect the physical integrity of the data center and the information resource systems residing within. Specifically, we evaluated the data center's access controls, environmental factors, and back-up procedures designed to ensure the continuity of AOC information technology operations.

This audit was included in the Fiscal Years 2018-2020 Office of Inspector General Audit Plan.

## Findings

Overall, the AOC developed and implemented policies and procedures to protect the physical integrity of the data center and the information resource systems residing within. Specifically, we determined that the Information Technology Division (ITD) complied with the requirements for the environmental factors and back-up procedures as prescribed by the AOC and other applicable guidance; however, the ITD lacked sufficient controls over physical access to the Data Center at the [REDACTED]. Specifically, we identified 35 AOC personnel that accessed the Data Center at the [REDACTED]. 10 were approved by and assigned to ITD and 25 were not.

The ITD should have a process in place for proper authorization and/or coordination with the U.S. Capitol Police (USCP) and other AOC jurisdictions to control physical access to the Data Center at the [REDACTED]. Without proper physical access controls for the Data Center at the [REDACTED], ITD's sensitive network computer equipment and technology may be at risk for unauthorized access, theft, or tampering.

In addition, AOC experienced a power outage at the [REDACTED] during the audit that caused some concerns. According to ITD officials, the effects of the power outage were minimal to the AOC due to the live replication of the [REDACTED] at the [REDACTED]. However, we found that a structured process was not in place for tenants to properly communicate and coordinate with the [REDACTED] Management.

According to the [REDACTED] management, communication and coordination with its tenants have been enhanced post power outage by providing monthly operational status updates and publishing emergency communication procedures. AOC officials should continue efforts to mitigate the risk of unplanned power outages and maintaining critical operations at its [REDACTED], the Data Center at the [REDACTED]. Due in part to a subsequent power outage at the [REDACTED], the ITD temporarily moved its primary operations from the [REDACTED] to the [REDACTED] Data Center for three months, though both sites were available for automatic failover as designed.

## Recommendations

We made two recommendations to address improvements to physical access controls.

1. 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; and
2. The Chief Information Officer enhance its communications and coordination with USCP and other AOC jurisdictions to improve physical access controls to the Data Center at the [REDACTED] for non-ITD personnel.



## Management Comments

└

## *Recommendations Table*

MANAGEMENT	RECOMMENDATIONS UNRESOLVED	RECOMMENDATIONS RESOLVED	RECOMMENDATIONS CLOSED
Architect of the Capitol, Chief Information Officer	None	A.1 and A.2	A.1 and A.2

Please provide Management's Decision by March 27, 2020

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 recommendation.

**RESOLVED** – Management agreed to implement the recommendation or has proposed action that will address the underlying finding that generated the recommendation.

**CLOSED** – OIG verified that the agreed upon corrective actions were implemented.



**Office of Inspector General**  
499 South Capitol Street, SW, Suite 518  
Washington, DC 20515  
202.593.1948  
  
www.aoc.gov

United States Government

## MEMORANDUM

**DATE:** September 27, 2019

**TO:** Thomas J. Carroll III,  
Acting Architect of the Capitol

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

**SUBJECT:** Audit of the Architect of the Capitol (AOC) Data Center

This memorandum transmits the final OIG Report OIG-AUD-2019-04 on the AOC Data Center audit.

AOC management agreed with the Office of Inspector General's (OIG's) conclusion that the Information Technology Division (ITD) lacked sufficient control over physical access to the Data Center at the [REDACTED] ([REDACTED] AOC management concurred with the two recommendations in this report.

AOC management implemented the recommendations on September 3, 2019. The OIG reviewed the AOC's revised Standard Operating Procedures for ITD Authorized Data Center Proxy Card Access List Maintenance to account for non-ITD personnel, and the memorandum from the Chief Information Officer on its communications and coordination with U.S. Capitol Police and other AOC jurisdictions to improve physical access controls to the Data Centers for non-ITD personnel. Therefore, the OIG considers the two recommendations to be closed.

We appreciate the courtesies extended to the staff during the audit. Please direct concerns and questions to Erica Wardley, Assistant Inspector General for Audits at 202.593.0081 or Erica.Wardley@aoc.gov.

Distribution List:

William O'Donnell, Chief Administrative Officer

Jay Wiegmann, Chief Information Officer

Valerie Hasberry, Acting Director, Office of Security Programs

Jason Baltimore, General Counsel

Mary Jean Pajak, Senior Advisor to the Chief Operating Officer

# Contents

---

<b>Results In Brief</b> .....	<b>i</b>
<u>Objective</u> .....	<u>1</u>
<u>Findings</u> .....	<u>1</u>
<u>Recommendations</u> .....	<u>1</u>
<u>Management Comments</u> .....	<u>ii</u>
<b>Introduction</b> .....	<b>1</b>
<u>Objective</u> .....	<u>1</u>
<u>Background</u> .....	<u>1</u>
<u>Criteria</u> .....	<u>6</u>
<b>Audit Results</b> .....	<b>7</b>
<b>Finding A</b> .....	<b>8</b>
<u>Physical Access Controls to the Data Center at the [REDACTED] ([REDACTED])</u> .....	<u>8</u>
<u>Needs Improvement</u> .....	<u>8</u>
<u>Recommendations</u> .....	<u>9</u>
<b>Other Matters</b> .....	<b>10</b>
<b>Appendix A</b> .....	<b>13</b>
<u>Scope and Methodology</u> .....	<u>13</u>
<u>Review of Internal Controls</u> .....	<u>14</u>
<u>Use of Computer-Processed Data</u> .....	<u>15</u>
<u>Prior Coverage</u> .....	<u>15</u>
<b>Appendix B</b> .....	<b>18</b>
<u>Notification Letter</u> .....	<u>18</u>
<b>Appendix C</b> .....	<b>19</b>
<u>Management Comments</u> .....	<u>19</u>
<b>Acronyms and Abbreviations</b> .....	<b>21</b>

# Introduction

---

## Objective

This audit report presents the results of our audit of the Architect of the Capitol’s (AOC) Data Center at the [REDACTED] ([REDACTED]). The objective of the audit was to determine whether the AOC developed and implemented policies and procedures to protect the physical integrity of the data center and the information resource systems residing within. Specifically, we evaluated the data center’s access controls, environmental factors, and back-up procedures designed to ensure the continuity of AOC information technology (IT) operations.

We conducted this performance audit of the AOC Data Center at the [REDACTED] (also referred to as “AOC Data Center” or “Data Center at the [REDACTED] in [REDACTED] and [REDACTED]” from August 2018 through August 2019, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

See Appendix A for a discussion of the scope and methodology, review of internal controls, and prior audit coverage related to the objective.

## Background

[REDACTED] ([REDACTED])

In April 2005, the AOC purchased the office building known as the [REDACTED] and the surrounding land for \$63,000,000. The [REDACTED] consists of a two story building located on a 92-acre site in [REDACTED]. The building is 345,282 square feet. The property has approximately 80-120 daily on-site personnel, including cleaning personnel. The [REDACTED] primary tenants are the [REDACTED], [REDACTED], and AOC Data Center. The AOC Data Center takes up 1,902 square feet of the [REDACTED].

The [REDACTED] [REDACTED], and AOC [REDACTED] (operated by AOC’s IT Division, henceforth referred to as [REDACTED])



## Data Center's Access Controls

For data center operations at the [REDACTED] the ITD authorizes access and maintains the access list for ITD staff and contractors for permission to enter the space. The ITD Authorized Access List is reconciled with the USCP ITD list to validate access privileges. The ITD has an assigned ITD Proxy Card Access Manager who is responsible for managing access to the data centers. The ITD Proxy Card Access Manager is notified by an ITD supervisor or staff to grant or revoke access to the data center. The ITD Proxy Card Access Manager completes the USCP Security Access Control Form that is submitted to the USCP, who grants or revokes access, as requested, through the proxy card reader via the individual's badge number.

## Environmental Factors

The critical environment factors for the AOC Data Center were prescribed in the Service Level Agreement (SLA) with [REDACTED] Management. For example, the SLA outlined the temperature and humidity levels for the data centers, "all data center areas will remain between 68 and 78 degrees Fahrenheit, and relative humidity will remain between 40 percent and 50 percent." In addition, the ITD provided the DELL.COM environmental temperature and humidity specifications and requirements for the servers currently used in production which aligns with the SLA requirements.

## Back-up Procedures

The ITD data backup procedures for the data center were performed on a routine schedule. Per the ITD Backup Standard Operating Procedure, daily, weekly, or monthly snapshots were conducted on AOC files, servers, databases, and applications. The ITD has two job summary reports used to monitor backup and restore activities. These reports include codes that provide detail on whether the backup or restore was active, delayed, completed, completed with errors, completed with warnings, killed, failed, aged, not scheduled, not run, or committed. The summary reports are reviewed by engineers and errors are addressed immediately. Backup data is stored at the AOC and [REDACTED] Data Centers, respectively, as well as on the [REDACTED], AOC's off-site location.

## **[REDACTED] MANAGEMENT AND TENANT ROLES AND RESPONSIBILITIES**

The AOC via [REDACTED] Management has executed a Memorandum of Understanding (MOU) between the [REDACTED], and ITD which serves as a formal

agreement for the purpose of defining the terms and conditions for co-occupying the [REDACTED] to include:

- The facility will be used primarily to satisfy Legislative Branch business operations.
- The parties shall share the use of commonly available infrastructure resources. The AOC is responsible for facility infrastructure improvements and for the operations and maintenance of the facility. However, if any party has a specific requirement that the AOC cannot support, then the requesting party may provide funds, via transfer, to the AOC for execution of work to satisfy their need.
- Parties recognize the importance of proper facility maintenance to minimize the risk of unplanned facility outages and agree to support all such activities as required. Activities requiring mission impacts and outages will be supported, but will be coordinated to minimize any impacts to the greatest extent possible.
- Parties shall conduct long range planning for their respective missions and coordinate with AOC as required to meet their infrastructure requirements. Parties understand that significant infrastructure construction and alterations may require years of planning, design and construction, and is subject to the availability of funds.
- Parties are subject to all applicable safety, security and other rules, regulations and authorities, to include, but not limited to, the Congressional Accountability Act and USCP Board.

As part of the MOU, each tenant will execute a SLA to meet the needs of the representative operations. Key provisions within the [REDACTED] Management's SLA included the following:

#### Environmental:

The AOC will use reasonable efforts to ensure that the temperature of open space in all data center areas will remain between 68 and 78 degrees Fahrenheit, and relative humidity will remain between 40 percent and 50 percent. This commitment excludes localized conditions within a particular customer cabinet, cage, rack, or other enclosed space.

### Power Availability:

The AOC's goal is to provide continuous redundant power to data center cabinets, as required, through utility service providers, generators, UPS, and distribution architecture. However, it is understood that maintenance, upgrades, and other situations could possibly compromise redundancy and reliability of electrical and mechanical systems.

### Critical Maintenance:

The maintenance of critical utilities may be performed at any time to correct mechanical and electrical conditions that require immediate attention. Critical maintenance is defined as maintenance which is necessary to ensure life safety and/or property to prevent the loss or damage of critical electrical/mechanical infrastructure. Critical maintenance is performed at the discretion of the AOC. All reasonable efforts will be made to notify the tenants' designated point(s) of contact as soon as practicable under the circumstance. However, it is recognized that AOC may have to perform certain critical maintenance that may impact "tenants operations." The AOC will seek to minimize disruptions and operational impacts.

### Tenants Responsibilities:

The Tenants, i.e., the [REDACTED] and ITD will notify the AOC Facility Manager immediately of any changes that may require additional infrastructure.

Tenants will notify the AOC when installing additional equipment that requires additional electrical service. Tenants shall submit electrical load requirements and heat load information to the AOC and allow the AOC to determine if the current infrastructure can support the additional equipment. The advance notice requirements may vary depending on circumstances and type of work requested. An early AOC involvement will help for better planning.

1. Tenants will submit updated drawings of the data centers or floor plans (equipment layouts) to the AOC as soon as possible after changes are made.
2. Tenants will coordinate long range plans with the AOC as they become available at the beginning of concept stages for better planning.
3. Tenants are responsible for communicating any notifications of maintenance work or outages to their customers.

## Criteria

AOC Order 7-4, Information Technology Security, dated October 10, 2017, states that the AOC requires that covered persons protect AOC data and information systems.

AOC Order 8-2, Information Technology Management, dated December 2, 2013, designated the CIO through the ITD to provide security over AOC IT operations to include AOC Data Centers.

Standard Operating Procedures, ITD Authorized Data Center Proxy Card Access List Maintenance, dated January 29, 2015, specified control procedures for proxy card access list and access to the AOC Data Centers.

MOU and SLA between the AOC and the [REDACTED] Tenants, executed March 22, 2012, to accommodate the co-location and operation of certain functions within the [REDACTED] that enables [REDACTED]

[REDACTED].

## Audit Results

---

Overall, the AOC developed and implemented policies and procedures to protect the physical integrity of the data center and the information resource systems residing within. Specifically, we evaluated the Data Center at the [REDACTED] access controls, environmental factors, and data back-up procedures designed to ensure the continuity of AOC IT operations. We determined that the ITD complied with the requirements for the environmental factors and back-up procedures as prescribed by the AOC and other applicable guidance. However, physical access controls to the Data Center at the [REDACTED] needed improvements.

We identified 35 AOC personnel accessed the facility in Fiscal Year (FY) 2018. Based on our review of the 35 personnel who accessed the room, 10 were approved by and assigned to ITD and 25 were not.

In addition, the AOC experienced a power outage at the [REDACTED] during the audit that caused some concerns. We note that the power outage occurred outside the scope of this audit; however, the outage resulted in an AOC Data Center temporary shutdown which impacted all tenant data centers within the [REDACTED] to include the AOC Data Center. [REDACTED] Management acknowledged the need for repairs and maintenance. According to ITD officials, the effects of the power outage were minimal to the AOC due to the live replication of the backup data processed at the [REDACTED] Data Center. However, we found that a structured process was not in place for tenants to properly communicate and coordinate with [REDACTED] Management. According to [REDACTED] Management, communication and coordination with its tenants have been enhanced post power outage by providing monthly operational status updates and publishing emergency communication procedures.

It is our conclusion that with proper physical access controls, the ITD would reduce the risk for unauthorized access, theft, or tampering within its Data Center at the [REDACTED]. In addition, AOC officials should continue efforts to mitigate the risk of unplanned power outages and maintaining critical operations at its primary site, the Data Center at the [REDACTED]. Due in part to a subsequent power outage at the [REDACTED] the ITD temporarily moved its primary operations from the [REDACTED] to the [REDACTED] Data Center for three months, though both sites were available for automatic failover as designed.

We made two recommendations to address the improvement of physical access controls.

## Finding A

---

### Physical Access Controls to the Data Center at the

### ████████████████████ (██████) Needs

### Improvement

The ITD lacked sufficient control over physical access to the Data Center at the ██████. Specifically, we identified 35 AOC personnel that accessed the Data Center at the ██████ from October 1, 2017, through September 30, 2018. Based on our review, of the 35 personnel that accessed the room, 10 were approved by and assigned to ITD and 25 were not.

The ITD is responsible for the safety and security of the IT equipment in the AOC Data Center at the ██████. The ITD may authorize or revoke access to the AOC Data Center for only ITD staff and contractors. These individuals are maintained on the ITD Authorized Access List. The ITD used this master list to reconcile ITD personnel with the USCP access list, also referred to as the Clearance Definition Report.

We determined that although ITD's process for review and reconciliation of ITD personnel access of the AOC Data Center was sufficient, ITD acknowledged it has no control over approval of non-ITD personnel access to the data center. The Office of Security Programs and USCP have authority to approve and remove access to the AOC Data Center at the ██████ for non-ITD personnel. We found 25 non-ITD personnel had access to sensitive AOC computer equipment a total of 1,257 times in FY 2018. To obtain a complete listing of all personnel who accessed the AOC Data Center during FY 2018, we requested and reviewed the personnel access log generated by USCP Security Access Control System (SACS). The SACS logged the card number, personnel name, date and time accessed when individuals scanned their proxy access card to the electronic card reader to gain entry. The SACS logs contained 1,530 records of entry into the Data Center at the ██████. We sorted the 1,529 records by personnel name and determined 35 individuals gained access to the facility. We compared the 35 individuals to the USCP's approved personnel access report and ITD's Authorized Access List and determined that only 10 were approved by and assigned to the ITD, and 25 were not. To further validate our conclusion, an ITD manager reviewed the identified 25 personnel and confirmed they were not assigned to the ITD.

The USCP provided specific details on these non-ITD personnel, to include the purpose for access, job description, and jurisdiction. The 25 non-ITD personnel were Office of Security Programs engineers and maintenance mechanics, [REDACTED] staff, USCP officers, AOC Facility manager, and security guards. After review and consultation with the ITD on the position descriptions, there were no identified concerns with the access of these non-ITD personnel.

According to AOC Order 7-4, Information Technology Security, the Architect of the Capitol designates the CIO as the authorizing official to grant, suspend, revoke, and modify the authority to operate for all general support systems and applications under the AOC's authority or control. AOC Order 8-2, Information Technology Management designates the ITD as the primary operational IT organization supporting the CIO. The ITD manages the operation of the AOC's automated information systems to include the AOC Data Center operations. Therefore, the ITD's responsibility for safety and security of the AOC Data Center should not only account for ITD staff and contractors but for anyone accessing the AOC Data Center. We 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 using proxy card access.

The ITD should have a process in place for proper authorization and/or coordination with USCP and other AOC jurisdictions to control physical access to the Data Center at the [REDACTED]. Without proper physical access controls for the Data Center at the [REDACTED] ITD's sensitive network computer equipment and technology may be at risk for unauthorized access, theft, or tampering.

## **Recommendations**

### ***Recommendation A.1***

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-Information Technology Division personnel.

### ***AOC Comment***

Concur. The AOC has revised its Information Technology Division (ITD) Authorized Data Center Proxy Card Access List Maintenance Standard Operating

---

[REDACTED] for the office of security programs consolidated facility management contract, which provide maintenance, custodial services, landscaping, and client services for the [REDACTED] and [REDACTED].

Procedure to include non-ITD personnel, effective September 3, 2019, completing this recommendation.

### ***OIG Response***

We recognize the AOC's concurrence with the recommendation. The OIG reviewed the revised Standard Operating Procedures and considers the recommendation closed.

### ***Recommendation A.2***

We recommend that the Chief Information Officer enhance its communications and coordination with U.S. Capitol Police and other AOC jurisdictions to improve physical access controls to the Data Center at the [REDACTED] for non-Information Technology Division personnel.

### ***AOC Comment***

Concur. The AOC Chief Information Officer has corresponded with and subsequently submitted a memorandum to the AOC Office of Security Programs and the United States Capitol Police on September 4, 2019, establishing a revised process to improve physical access controls to the AOC data center at the [REDACTED] for non-ITD personnel.

### ***OIG Response***

We recognize the AOC's concurrence with the recommendation. The OIG reviewed AOC's communication memorandum and considers the recommendation closed.

## Other Matters

---

As an observation during the course of our audit, the [REDACTED] experienced a loss of power on October 8, 2018, which impacted all tenant data centers within the [REDACTED] to include the AOC Data Center. We conducted interviews with [REDACTED] Management officials responsible for the operations, maintenance, and security at the [REDACTED] and reviewed facility assessments and reports to gain a better understanding on what caused the power outage.

[REDACTED] Management officials (i) acknowledged the need for repairs and maintenance to the UPS, switchgears, chillers, air conditioning systems, and sprinkler systems; (ii) noted major construction needs such as chilled water system modernization, roof replacement, and fire suppression system modernization; and (iii) identified that the [REDACTED] with the Data Centers at the [REDACTED] were the back-up systems. The [REDACTED] is currently using [REDACTED]

It was determined that the [REDACTED] total loss of power was due to the failure of a lightning arrestor within the primary switchgear supporting the facility. The initial incident report documented that the building's life safety emergency generator operated as designed and provided power to the emergency lighting and life safety systems. The incident report further documented that the two stand-by generators for critical systems and three UPS failed to operate as designed. However, the report information was later revised in the [REDACTED] Outage Incident Information report, dated October 11, 2018. The revised information stated that "the facility did not automatically switch to generator power for the critical systems as designed and the generators did not automatically power the UPS systems as designed. This resulted in the eventual loss of all data centers in the [REDACTED]. The critical systems generators failed to operate automatically due to damage sustained as a result of the failed lightning arrestors. The generators were manually started but were not able to connect to data center loads due to damaged electronic systems. All data centers operated off of the UPS batteries for [REDACTED] until they were drained. Once the batteries drained, the data centers remained off-line until commercial power was restored.

After discussions with [REDACTED] Management, it was noted that the AOC had not provided adequate training for its personnel concerning emergency situations.

Subsequent to this power outage, [REDACTED] Management commissioned a third party to complete a facility asset management plan to report on areas of potential failure to

operational [REDACTED], current performance suggested improvements, Tier level requirements, and cost ranges to meet current data center needs. The report stated that the risk of cooling and electrical system failures are contributing to the overall risk of operational [REDACTED] and tier level goals of the [REDACTED]

The [REDACTED] Management has a SLA with its tenants to include the AOC Data Center that states the “goal...is to provide continuous redundant power to data center cabinets, as required, through utility service providers, generators, UPS, and distribution architecture. However it is understood that maintenance, upgrades and other situations could possibly compromise redundancy and reliability of electrical and mechanical systems.” In addition, the SLA states that “the maintenance of critical utilities may be performed at any time to correct mechanical and electrical conditions that require immediate attention. Critical maintenance is defined as maintenance which is necessary to ensure life safety and/or property to prevent the loss or damage of critical electrical/mechanical infrastructure. All reasonable efforts will be made to notify the tenants' designated point of contacts as soon as practicable under the circumstance. However, it is recognized that the AOC may have to perform certain critical maintenance that may impact ‘tenants operations’.”

We found that a structured process was not in place for tenants to properly communicate and coordinate with the [REDACTED] Management. Per ITD officials, [REDACTED] Management did not regularly inform ITD of operational status performance measures and indicators. The [REDACTED] Management also acknowledged that inadequate communication with CIOs and other stakeholders regarding facility maintenance and repair operations were reported as major tenant concerns. Per [REDACTED] Management officials, [REDACTED] Management is now providing monthly operational status updates to ITD staff along with the other tenants. The [REDACTED] also published an emergency communications Standard Operating Procedures to contact data centers managers in case of an emergency. These standard operating procedures should reduce the notification time to facility managers and key stakeholders from hours to minutes. The [REDACTED] Management has also taken steps to address key infrastructure shortfalls by completing facility needs assessments to augment future year funding requests.

According to the [REDACTED] analysis<sup>2</sup>, the Data Center at the [REDACTED] IT infrastructure, design, and support/management processes are capable of providing for current needs, as well as expected 3-5 year workload growth demands in concert with the capabilities of the [REDACTED] Data Center. However, AOC officials should continue efforts to mitigate the risk of unplanned power outages and maintaining critical operations at its primary site.

---

<sup>2</sup> Data Center Review, Requirements, and Cost Benefit Analysis Prepared for the [REDACTED], prepared by [REDACTED] DATED March 22, 2017.

# Appendix A

---

## Scope and Methodology

The scope of this performance audit was October 1, 2017, through September 30, 2018. The audit scope was limited to the AOC Data Center at the [REDACTED]. We conducted this performance audit of AOC ITD located in [REDACTED] and [REDACTED] from August 2018 through July 2019, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To determine whether the AOC developed and implemented policies and procedures to protect the physical integrity of the data center and the information resource systems residing we interviewed and had discussions with key personnel from the Office of IT, Office of Security Programs and the USCP. We reviewed public law 107-347; the AOC's Information Technology Order 7-4 Order 8-2; Federal Information Processing Standards Publication 200; ITD Data Center Proxy Card Access Card Procedures; MOU between the AOC and the USCP; and the [REDACTED] SLA between the AOC and Occupants.

We tested the data center's access controls, environmental factors, and data back-up procedures designed to ensure the continuity of AOC IT operations.

### *Access Controls*

We obtained a complete list of all individuals who accessed the AOC Data Center during FY 2018 and we requested and reviewed the personnel access log generated by USCP Security Access Control System for the period.

### *Environmental Factors*

We obtained and reviewed the Daily Operational and Status Dashboard reports. These reports detail the daily data center room temperatures and relative humidity. We compared the compiled information to the environmental standards for data centers in the American Society of Heating, Refrigeration, and Air Conditioning Engineers and the AOC's SLA.

### *Backup Procedures*

We reviewed the ITD Backup standard operating procedures, dated June 26, 2018, which describes the current Backup Procedure for Files, Server, Database and Application Backup; Backup Data Retention; and Restore and Maintenance. We reviewed ITD's Job Summary Reports Backup for the period of June 4, 2018, through October 1, 2018.

This audit was included in the FYs 2018-2020 Office of Inspector General Audit and Evaluation Plan.

## **Review of Internal Controls**

Government Auditing Standards requires auditors to obtain an understanding of internal control that is significant within the context of the audit objectives. For internal controls that are significant within the context of the audit objectives, auditors should assess whether the internal control has been properly designed and implemented and should perform procedures designed to obtain sufficient and appropriate evidence to support their assessment about the effectiveness of those controls. Information system controls are often an integral part of an entity's internal control. The effectiveness of significant internal controls is frequently dependent on the effectiveness of information systems controls. Thus, when obtaining an understanding of internal control significant to the audit objectives, auditors should also determine whether it is necessary to evaluate information systems controls.

We reviewed internal controls to obtain an understanding of the AOC's Data Center access controls and back-up procedures designed to ensure the continuity of AOC IT operations. We obtained our understanding by reviewing the applicable laws, regulations, and AOC policies to determine (i) the roles and responsibilities for physical access control and uninterruptable power, and (ii) if controls, individually or in combination with others controls, were properly implemented and working as designed.

The AOC Orders 4-10, Internal Controls Program, 7-4, Information Technology Security 8-2, Information Technology Management, ITD Backup Procedure and ITD Proxy Access Card Access List Standard Operating Procedures documented uniform policies for AOC staff to ensure conformity with the written terms, conditions and specifications of the MOU. Although ITD's process for back-up procedures and review and reconciliation of ITD personnel access of the AOC Data Center was sufficient, ITD acknowledged it has no control over approval of non-ITD personnel access to the data center.

## Use of Computer-Processed Data

We used a material amount of computer-processed data to perform this audit. The computer processed data relates to physical access controls to the AOC Data Center at the [REDACTED] and ITD server system back-up and restore job summary reports.

The computer processed data for physical access controls was Data Center access logs from October 1, 2017 through September 30, 2018. The access logs were extracted from the security access control system maintained by the USCP. The USCP OIG conducted two performance audits, in 2015 and 2018, of USCP controls over proximity cards, which include testing of controls and validation of data surrounding the Security Access Control System. However, due to the law enforcement sensitivity of the reports, the USCP did not share the reports. The data was compared to source documentation and confirmed by the USCP. Based on our understanding of the security access control system and the reliability determined by the USCP OIG audit, we can conclude that the computer processed data provided by the USCP regarding personnel access to the AOC Data Center at the [REDACTED] is sufficiently reliable for the purposes of our audit.

The computer processed data for back-up procedures was weekly Back-Up Summary Reports and monthly Restore Job Summary Reports. The ITD utilized commercial software to generate these reports. We obtained and reviewed the system software overview and conducted interviews with ITD staff to gain a detailed understanding of the software. We reviewed the ITD's report criteria and verified that each generated report contained the same criteria to ensure the completeness of the reports. In addition, we reviewed system generated email notifications used to confirm network back-up. Therefore, we concluded that the computer processed data provided was sufficiently reliable for the purposes of our audit.

## Prior Coverage

During the last five years, the AOC OIG and House OIG issued two reports discussing matters related to AOC Data Center Access.

### *AOC OIG*

Report No. A-2015-03 "AOC report on the [REDACTED] Data Center Access"

The objective of the review was to determine whether the list of 18 AOC employees identified as no longer authorized access were actually removed from the access records. Facility managers from the House Information

Resources and AOC Jurisdictions responsible for personnel access and removal did not remove 18 personnel that were no longer AOC employees or contractors. This occurred because Jurisdictions, primarily the construction division, did not recover identification badges from the departing employees as required.

The report recommended the removal of the 18 employees or contractors from the House CAO and USCP access list and regular review of AOC employee access records and compliance with AOC order 296-4.

## ***HOUSE OIG***

Report No. 14-AOC-17 "Audit of the Architect of the Capitol's Information Technology Risk Management Framework"

The objective of the audit was to evaluate the AOC Risk Management Framework implementation and risk management activities, specifically, those related to disaster recovery, to ensure that AOC security controls are adequately documented, validated and operating effectively. The audit team reviewed and compared AOC policies and procedures with industry best practices and examined compliance with those policies and procedures. The report determined that while the AOC maintains an internal list of AOC Information Technology Division (ITD) personnel that have access to AOC Data Centers, the AOC does not reconcile this list with USCP authorized access lists produced from the proximity card system of record.

One of 20 AOC ITD employees/contractors on the USCP authorized access list provided by the AOC had not worked for the AOC since January of 2013. While the AOC submitted an access revocation request to the USCP for this individual upon their separation; the AOC did not detect that the request was not completed. Additionally, the AOC was unable to provide documentation to demonstrate this individual's ID badge was collected upon separation. The ID badge remained active for 90 days after separating from the AOC.

14 of 27 AOC ITD employees/contractors listed on the AOC's ITD authorized access list were not on the USCP authorized access list.

Management concurred with the recommendation and stated AOC is updating the ITD authorized access list so that it accurately reflects ITD employees/contractors access to data center and is implementing controls to ensure the list is properly maintained. The full list will be provided to the House Information Resources at least quarterly. As ITD personnel leave the

AOC, the ITD designated points of contact will notify HIR. The updated ITD authorized access list is scheduled to be completed November 2014. Final Action - the AOC ITD authorized access list has been updated and controls implemented for its maintenance.

# Appendix B

## Notification Letter



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

United States Government

### MEMORANDUM

DATE: August 20, 2018

TO: Stephen T. Ayers, FAIA, LEED AP  
Architect of the Capitol

FROM: Christopher P. Failla   
Inspector General

SUBJECT: Architect of the Capitol (AOC) Data Center Audit  
(2018-0012-AUD-P)

This memorandum serves as notification that the Office of Inspector General plans to initiate an audit of the AOC Data Center. Our objective is to determine whether the AOC has developed and implemented policies and procedures to protect the physical integrity of the data center and the information resource systems residing within. Specifically, we will evaluate the data center's access controls, environmental factors, and back-up procedures designed to ensure the continuity of AOC information technology operations. We will limit our scope to the AOC Data Center at the [REDACTED].

We will contact you to set up an entrance conference. If you have any questions, please contact Paul Braxton at 202.593.0107 or MaryAnn Davenport at 202.593.0081.

Distribution List:

Christine A. Merdon, P.E., CCM, Chief Operating Officer  
Dan Cassil, Chief Administrative Officer  
Jay Wiegmann, Chief Information Officer  
Shalley Kim, Executive Officer  
Mary Jean Pajak, Senior Advisor to the Chief Operating Officer  
James Drummond, Assistant Director, Facilities Management Division

# Appendix C

## Management Comments



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

United States Government

### MEMORANDUM

DATE: September 12, 2019  
TO: Christopher P. Failla, Inspector General  
FROM: Thomas J. Carroll III   
Acting Architect of the Capitol  
SUBJECT: Draft Report Audit of Architect of the Capitol Data Center (2018-012-AUD-P)

Thank you for the opportunity to review and comment on the subject draft report regarding the Architect of the Capitol (AOC) Data Center at the [REDACTED].

The following comments on the subject report's finding and recommendations are provided:

**OIG Finding A:** Physical Access Controls to the Data Center at the [REDACTED] ( [REDACTED] ) Needs Improvement.

**AOC Comment:** Concur. The AOC agrees with the finding, and has completed the two associated recommendations, as documented below, to improve physical access controls to its data center at the [REDACTED].

**OIG Recommendation One:** 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.

**AOC Comment:** Concur. The AOC has revised its Information Technology Division (ITD) Authorized Data Center Proxy Card Access List Maintenance Standard Operating Procedure to include non-ITD personnel, effective September 3, 2019, completing this recommendation.

**OIG Recommendation Two:** The Chief Information Officer enhance its communications and coordination with USCP and other AOC jurisdictions to improve physical access controls to the Data Center at the [REDACTED] for non-ITD personnel.

**AOC Comment:** Concur. The AOC Chief Information Officer has corresponded with and subsequently submitted a memorandum to the AOC Office of Security Programs and the United States Capitol Police on September 4, 2019, establishing a revised process to improve physical access controls to the AOC data center at the [REDACTED] for non-ITD personnel. We believe these actions and new process complete the recommendation.

Thank you for the opportunity to provide comments to the draft report. Please contact William O'Donnell, AOC Chief Administrative Officer, by telephone at 202.226.0007 or electronic mail at [william.odonnell@aoe.gov](mailto:william.odonnell@aoe.gov) if there are any questions.

Doc. No. 190904-02-01

# Acronyms and Abbreviations

---

AOC	Architect of the Capitol
█	█
CIO	Chief Information Officer
FY	Fiscal Year
LOC	Library of Congress
IT	Information Technology
ITD	Information Technology Division
MOU	Memorandum of Understanding
OIG	Office of the Inspector General
SACS	Security Access Control System
SLA	Service Level Agreement
UPS	Uninterrupted Power Supplies
USCP	United States Capitol Police



INSPECTOR GENERAL  
499 S. CAPITOL STREET, SW  
SUITE 518  
WASHINGTON, D.C 20515  
[www.aoc.gov](http://www.aoc.gov)