DeKalb County
GEORGIA

Office of Independent Internal Audit

LAVOIS CAMPBELL, CHIEF AUDIT EXECUT IV E

FINAL

February 22, 2023

John Matelski,
Chief Innovation & Information Officer
Department of Innovation & Technology

RE: Data Center Physical Security Audit, Audit Report Number 2018-007-IT - Audit Follow-up Report

Dear Mr. Matelski,

As required by DeKalb County, Georgia – Code of Ordinances/Organizational Act Section10A-Independent Internal Audit (I), I have attached the Office of Independent Internal Audit's (OIIA) report on the status of management actions taken to address the findings contained in the referenced audit report. The conclusions in this follow-up report are limited to the status of the implementation and not the effectiveness of the completed action plans, which may be assessed in a future audit.

On June 29, 2021, our office performed an initial assessment of the status of management action plans to address the 17 findings noted in the confidential audit report. At that time action plans for ten (10) of the 17 findings were assessed as closed/completed and seven were assessed as either "open" or "partially complete". This report provides the result of our subsequent follow-up to verify the status of management action plans to address the remaining seven findings that were either "Open" or "Partially Complete". The current status of the remaining seven findings is indicated in the table below.

Management is working through the process of completing all the corrective actions. They have indicated Q4, 2023 as the anticipated timeline to complete the action plans. We will follow up after that date to verify the completion of the plans.

Figure 1 - Status of Management Actions Plans

Finding No.	Report Finding	Status of Management Action Plans
1	CONFIDENTIAL	Partially Complete
3	Non-enforcement of Data Center Site Inspection.	Closed
7	CONFIDENTIAL	Partially Complete
9	Access Management (badge administration) Needs Improvement	Closed
13	Disaster Recovery Plan for Vital Support Systems within the Data Center Needs Improvement.	Closed
15	The Data Backup Software Needs Upgrade.	Closed
16	Security Awareness Training Needs Improvement.	Closed

Please contact me if you require additional information.

Regards,

Lavois Campbell
Lavois Campbell, CIA, CISA, CFE, CGA-CPA
Chief Audit Executive

Attachment: Audit Findings Status Update Form

cc. Michael L. Thurmond, Chief Executive Officer

Robert Patrick, Board of Commissioners District 1
Michelle Long Spears, Board of Commissioners District 2
Larry Johnson, Board of Commissioners District 3
Steve Bradshaw, Board of Commissioners District 4
Mereda Davis Johnson, Board of Commissioners District 5
Ted Terry, Board of Commissioners District 6
Lorraine Cochran-Johnson, Board of Commissioners District 7
Lisa Earls, Chairperson, Audit Oversight Committee
Gloria G. Gray, Vice-Chairperson, Audit Oversight Committee,
Tanja Christine Boyd-Witherspoon, Pro-Tem, Audit Oversight Committee
Adrienne T. McMillion, Audit Oversight Committee
Harold Smith Jr., Audit Oversight Committee
La'Keitha D. Carlos, CEO's Chief of Staff
Kwasi K. Obeng, Chief of Staff, Board of Commissioners
Michelle Butler, Chief Procurement Officer (Interim)

Office of Independent Internal Audit

LAVOIS CAMPBELL, CHIEF AUDIT EXECUT IV E

FINAL

DeKalb County Government

Office of Independent Internal Audit

Date: 2/16/2023 **Prepared by: Rubby Ibe-Ikechi**

Audit Findings Status Update Form

Status Date	Report #	Report Title
2/16/23	2018-007-IT	Audit Of DeKalb County Data Center Physical Security

Contact Person	Title	Phone No.	Email Address
John Matelski	Chief Innovation & Information Officer	(404) 371-6210	jmatelski@dekalbcountyga.gov

Activity	Accountability	Schedule	
	Responsible Area	Repeat Finding	Anticipated Completion Date/Date Adjustments will be made
Follow-Up	Data Center Usage Policy/Agreement		**N/A**

Finding		Finding Detail
No.	#1	
Date	8/14/19	

Finding	**CONFIDENTIAL**
Recommendation	**Note:** The details of this finding are confidential under the exemptions noted in Georgia Open Records Act #50-18-70. The details of this finding would put the organization at risk. Questions and further information should be requested from the Chief Audit Executive of the Office of the Independent Internal Audit.
Management Response	**CONFIDENTIAL**
Second Status Update ☐ Open ☐ Management/Agency Assumes Risk ☒ Partially Complete ☐ Complete Pending Verification by OIIA ☐ Closed	**CONFIDENTIAL**

Office of Independent Internal Audit

LAVOIS CAMPBELL, CHIEF AUDIT EXECUT IV E

FINAL

DeKalb County Government

Office of Independent Internal Audit

Date: 2/16/2023 **Prepared by: Rubby Ibe-Ikechi**

Audit Findings Status Update Form

Status Date	Report #	Report Title
2/16/23	2018-007-IT	Audit Of DeKalb County Data Center Physical Security

Contact Person	Title	Phone No.	Email Address
John Matelski	Chief Innovation & Information Officer	(404) 371-6210	jmatelski@dekalbcountyga.gov

Activity	Accountability	Schedule	
	Responsible Area	**Repeat Finding**	**Anticipated Completion Date/Date Adjustments will be made**
Follow-Up	Data Center Site Inspection Enforcement		**N/A**

Finding		Finding Detail
No.	**#3**	
Date	**8/14/19**	

Finding	During the audit, we noted some procedures and documentation regarding data center site inspections performed by the information security staff. However, discussions with DoIT management revealed that these inspections are not always performed because of limited resources and time constraints.
Recommendation	We recommend that management re-implement this procedure along with communication to the CEO to help ensure that sufficient measures are in place to protect the physical security of the data center.
Management Response	DoIT has not performed any formal inspections recently, as there are systems deployed to advise when anomalies or issues occur in the data center. Automated systems provide real-time feedback, and as issues occur, DoIT staff is dispatched to investigate and resolve. DoIT will enhance its current automated protocols by scheduling additional monthly walk-through inspections. This procedure is now in place effective immediately.

Second Status Update	
□	Open
□	Management/Agency Assumes Risk
□	Partially Complete
□	Complete Pending Verification by OIIA
X	Closed

Status Response as at 6-29-2021: DoIT implemented a procedure by year-end 2019 whereby both data centers were visited and inspected on a weekly basis. When the COVID-19 pandemic hit, these site visits were halted as the facilities are technically closed. DoIT is mounting cameras to facilitate constant monitoring and "inspection" and will have them in place by the end of January 2021.

Status Response as at 2-16-2023: Completed.

Office of Independent Internal Audit

LAVOIS CAMPBELL, CHIEF AUDIT EXECUT IV E

FINAL

DeKalb County Government			
Office of Independent Internal Audit			
Date: 2/16/2023			**Prepared by: Rubby Ibe-Ikechi**
Audit Findings Status Update Form			

Status Date	**Report #**	**Report Title**
2/16/23	2018-007-IT	Audit Of DeKalb County Data Center Physical Security

Contact Person	**Title**	**Phone No.**	**Email Address**
John Matelski	Chief Innovation & Information Officer	(404) 371-6210	jmatelski@dekalbcountyga.gov

Activity	**Accountability**	**Schedule**	
Follow-Up	**Responsible Area**	**Repeat Finding**	**Anticipated Completion Date/Date Adjustments will be made**
	Environmental Security		**Continuous Improvement**

Finding		**Finding Detail**
No.	**#7**	
Date	**8/14/19**	
Finding		**CONFIDENTIAL**
Recommendation		**Note:** The details of this finding are confidential under the exemptions noted in Georgia Open Records Act #50-18-70. The details of this finding would put the organization at risk. Questions and further information should be requested from the Chief Audit Executive of the Office of the Independent Internal Audit.
Management Response		**CONFIDENTIAL**
Status Update-12 months		**CONFIDENTIAL**
□	Open	
□	Management/Agency Assumes Risk	
☒	Partially Complete	
□	Complete Pending Verification by OIIA	
□	Closed	

DeKalb County Government	
Office of Independent Internal Audit	
Date: 2/16/2023	**Prepared by: Rubby Ibe-Ikechi**

Audit Findings Status Update Form

Status Date	Report #	Report Title
2/16/23	2018-007-IT	Audit Of DeKalb County Data Center Physical Security

Contact Person	Title	Phone No.	Email Address
John Matelski	Chief Innovation & Information Officer	(404) 371-6210	jmatelski@dekalbcountyga.gov

Activity	Accountability	Schedule	
Follow-Up	**Responsible Area**	**Repeat Finding**	**Anticipated Completion Date/Date Adjustments will be made**
	Access Management		**N/A**

Finding		Finding Detail
No.	**#9**	
Date	**8/14/19**	

Finding	During the audit, we noted several areas related to access management and control that need improvement. •Since the data centers are located in buildings that are managed by other departments, authorizing and approving access to the data center is not always controlled by DoIT management. This means that DoIT is not able to ensure that access to the data center is only granted through the authorizing officials stated in the Physical Security policy. •Procedures for performing access reviews were not documented and the evidence of previous reviews was either incomplete or had not been maintained. In addition, there was no evidence that vendor access review has been performed. •DoIT did not consistently monitor data center access transaction reports and did not always document transaction report review. Further, there was no evidence that multiple failed attempts were investigated. •The authorized access list for the data center noted three users who had been authorized to have access but had not been added to the Authorized IT Personnel list. In addition, we noted one user who had terminated but remained on the list of authorized personnel and the badge was still active. In one instance the employee had retired in 2000 and the security reports indicate that badge had unsuccessfully attempted access to the data center location at the Courthouse.
Recommendation	We recommend that management: •Develop written policies for governing, granting and removing access to the data centers that include all of the departments who would be required to access the data centers. •Develop specific procedures to monitor access controls and establish a frequency for periodic access reviews based the risks in the current environment. These procedures should also include, but not be limited to, the following: •Documentation of access-related control activities. •Roles, responsibilities, and documentation for the access review. •Reporting the results of access review to all areas responsible for managing the data center. This report should include action plans to resolve any issues identified.
Management Response	DoIT has identified distributed access control as a risk since the current leadership team began working at the county. We do leverage policies and procedures that have been developed under the National Institute of Technology (NIST) Cyber Security Framework (CSF), however because IT does not have official authority to mandate compliance, this continues to be a challenge. DoIT will work with the Administration to shore up the written policies and enforcement capabilities associated with this recommendation. Full implementation of this recommendation will require support from senior leadership of the Sheriff's Office, Police Department and Facilities Management. Progress will be made over the next 6 months toward this end.

Second Status Update		
☐	Open	**<u>Status Response as at 6-29-2021:</u>** DoIT has a formal arrangement in place, and has had discussions with all stakeholders. Unfortunately, some of the constitutional officers believe that because the data center is in THEIR building, that they must have ANY of their staff members with access, and are unwilling to change their procedures. They are claiming a public safety exemption. **<u>Status Response as at 2-16-2023:</u>** Same response as above. An updated policy version has been provided via email.
☐	Management/Agency Assumes Risk	
☐	Partially Complete	
☐	Complete Pending Verification by OIIA	
X	Closed	

Office of Independent Internal Audit

LAVOIS CAMPBELL, CHIEF AUDIT EXECUT IV E

FINAL

DeKalb County Government

Office of Independent Internal Audit

Date: 2/16/2023 **Prepared by: Rubby Ibe-Ikechi**

Audit Findings Status Update Form

Status Date	Report #	Report Title
2/16/23	2018-007-IT	Audit Of DeKalb County Data Center Physical Security

Contact Person	Title	Phone No.	Email Address
John Matelski	Chief Innovation & Information Officer	(404) 371-6210	jmatelski@dekalbcountyga.gov

Activity	Accountability	Schedule	
	Responsible Area	**Repeat Finding**	**Anticipated Completion Date/Date Adjustments will be made**
Follow-Up	Disaster Recovery Plan		**N/A**

Finding	
No. **#13** **Date** **8/14/19**	**Finding Detail**
Finding	Management did not provide a disaster recovery plan as a part of the policies and procedures shared during the audit. Although a Business Continuity Plan was obtained, it did not contain the specific components or information regarding how the IT would restore vital support systems within the data center should a disaster occurred.
Recommendation	We recommend that management create a DRP for the County's critical IT infrastructure. At a minimum, this should include: •Disaster recovery policies and procedures •A business impact analysis (BIA), a disaster recovery strategy, recovery time objectives (RTOs), recovery point objectives (RPOs), resources and materials needed to recover the County's system. •DR Team including roles & responsibilities. •Complete and accurate infrastructure documentation. •End-to-end recovery processes to recover infrastructure and associated applications, system backup/restore, DR Team and Task. •End-to-end testing, validation and reporting.
Management Response	DoIT will coordinate to enhance the Disaster Recovery plan. DoIT leverages policies and procedures that have been developed under the National Institute of Technology (NIST) Cyber Security Framework (CSF). Based on this Audit recommendation, DoIT will tweak its Continuity of Operations and Disaster Recovery plans to address the concerns cited in this audit finding. These enhancements will be completed by end of first quarter 2020.
Second Status Update ☐ Open ☐ Management/Agency Assumes Risk ☐ Partially Complete ☐ Complete Pending Verification by OIIA X Closed	**Status Response as at 6-29-2021:** A consolidated Continuity of Operations and Business continuity plan is managed and coordinated by DEMA, and DoIT works closely with them to ensure that it is up to date from an enterprise perspective, as well as collaborating with departments/agencies on their individual plans as well. Disaster recovery is a subset of business continuity, and is covered by all existing DoIT supporting policies and procedures developed under the NIST CSF. **Status Response as at 2-16-2023:** The COOP is in process of being updated again, to take into account many system modernizations that occurred as a result of the pandemic. All of the annexes require updating. It is DoIT's intent to have the annexes updated by end of 2nd Quarter 2023.

FINAL

DeKalb County Government			
Office of Independent Internal Audit			
Date: 2/16/2023		**Prepared by: Rubby Ibe-Ikechi**	
Audit Findings Status Update Form			
Status Date	**Report #**	**Report Title**	
2/16/23	2018-007-IT	Audit Of DeKalb County Data Center Physical Security	
Contact Person	**Title**	**Phone No.**	**Email Address**
John Matelski	Chief Innovation & Information Officer	(404) 371-6210	jmatelski@dekalbcountyga.gov
Activity	**Accountability**	**Schedule**	
Follow-Up	**Responsible Area**	**Repeat Finding**	**Anticipated Completion Date/Date Adjustments will be made**
	Data Backup Software		**N/A**

Finding		**Finding Detail**
No.	**#15**	
Date	**8/14/19**	
Finding		The audit found that that all backups are performed using the Veritas NetBackup Enterprise Server version 7.7. This backup software version is in the End of Life process. The end of the standard support date was May 5, 2019. At this point the vendor has stopped delivering standard support for the product. Traditionally, this includes voice and electronic technical support, software upgrades, support for new and known defects (service packs and updates).
Recommendation		We recommend that management implement a plan for the system's life cycle, eventual end of life, and any corresponding security and business impacts.
Management Response		DoIT has been researching viable system replacements and has been approved for funding to modernize backup systems. The new system will be implemented no later than end of first quarter 2020, and likely will be in place by year-end 2019 if everything goes as planned.

Second Status Update		**<u>Status Response as at 6-29-2021:</u>** DoIT is in the process of modernizing our backup systems, and should be fully implemented by end of Q1 2021. **<u>Status Response as at 2-16-2023:</u>** Completed.
	Open	
	Management/Agency Assumes Risk	
	Partially Complete	
	Complete Pending Verification by OIIA	
X	Closed	

DeKalb County Government			
Office of Independent Internal Audit			
Date: 2/16/2023			**Prepared by: Rubby Ibe-Ikechi**
Audit Findings Status Update Form			

Status Date	**Report #**	**Report Title**
2/16/23	2018-007-IT	Audit Of DeKalb County Data Center Physical Security

Contact Person	**Title**	**Phone No.**	**Email Address**
John Matelski	Chief Innovation & Information Officer	(404) 371-6210	jmatelski@dekalbcountyga.gov

Activity	**Accountability**	**Schedule**	
Follow-Up	**Responsible Area**	**Repeat Finding**	**Anticipated Completion Date/Date Adjustments will be made**
	Security Awareness Training		**N/A**

Finding		**Finding Detail**
No.	**#16**	
Date	**8/14/19**	

Finding	The Department of Innovation & Technology has various training and awareness activities that included components of IT security, for example Georgia Crime Information Center (GCIC) Security Awareness training course. However, the audit found that these activities were not mandatory or scheduled on a periodic basis, nor is it clear whether these activities provide comprehensive coverage of key IT security responsibilities and there was no evidence that training has been completed by all employees.
Recommendation	We recommend that management establish a formal security awareness training program that includes details of the policies and procedures staff must follow, guidance on escalation and roles and responsibilities. Evidence of a formal training record should be maintained.
Management Response	DoIT has a fairly robust training program in place which includes some level of training/education that start during New Employee Orientation. Additionally, daily, weekly and monthly education is provided via email. That having been said, there is room to improve and expand. DoIT is developing an interactive training module specific to IT Security and will be rolling that training out no later than 1st quarter 2020. This training will allow for tracking employees who completed the training, and allow for follow-up for those who do not.
Second Status Update □ Open □ Management/Agency Assumes Risk □ Partially Complete □ Complete Pending Verification by OIIA ☒ Closed	**<u>Status Response as at 6-29-2021:</u>** DoIT has coordinated with HR and updated on-boarding training to include primers regarding acceptable use of county systems. DoIT provided county wide cyber security related training, which concluded in a quiz that needed to be passed. Unfortunately, certain agencies chose to allow their employees to opt out, and DoIT has no enforcement authority to compel compliance. **<u>Status Response as at 2-16-2023:</u>** Replacing old system with a system that can assess cyber readiness through real time phishing etc... activities. Those people who need to be trained based on their cyber hygeine habits, will receive training through this new system.