Cobb County...Expect the Best!

INTERNAL AUDIT DEPARTMENT

Report Number: 2022-007

Follow-up Report – Network Security Audit

(Performed by RSM US, LLP[1])

August 26, 2022

Latona Thomas, CPA, CIA, Director
Erica Brooks Peters, CPA

[1] RSM US, LLP is a vendor selected through the County's selection process to perform supplemental internal auditing services. [Source: Cobb County Contract No. 18955, dated April 21, 2020]

Executive Summary

Objectives & Scope

The purpose of this review was to revisit the Q1 2021 assessment of domains associated the County's network security processes and technology while providing a status on the recommendations from the original Report #2021-001, dated February 23, 2021.

- **Domains Revisited**: Certificate Management, Email Protection, Filter Network Traffic, Multi-Factor Authentication (MFA), Network Intrusion Prevention, Exploit Protection, and Security Information and Event Management (SIEM).

Review Summary

During the Q3 2022 review, RSM noted the below summarized results.

- Of the 19 observations made by RSM in 2021, 14 have been addressed through technology and process enhancement. Addressed observations include the higher priority items associated with MFA, recommended by RSM in 2021.
- For the remaining 5 observations, the County has projects in progress to evaluate and enable solutions.

Enhancement Roadmap

Various internal initiatives underway at the County, refer to 'Projects in Progress' section for additional details.

- **DLP**: Email and internal network traffic analysis
- **Policy Enhancement**: Incident response plan and certificate management
- **SIEM Program**: Finalization and documentation of enabling processes, including exception management

© 2022 RSM US LLP. All Rights Reserved.

Summarized Enhancements

- The County has updated policies and standards to reflect enhancements and is in the process of publishing them to all County technology users for acknowledgement with knowledge testing.
- All County technology employees have been enrolled in MFA, with special provisions for administrators.
- Network filtering capabilities have been matured, including IPS configuration, restriction of permitted ports/protocols, and enrollment of DDOS mitigation services.
- Log retention and associated backups have been increased to over a year (from 7–14 days).
- As part of the data center refresh, IPS (firewall) locations have been included in network diagrams.
- Through procurement of new technology, the County has increased email protection capabilities.

© 2022 RSM US LLP. All Rights Reserved.