The Maryland-National Capital Park and Planning Commission
Office of the Inspector General

eDiscovery Audit
Report Number: CW-005-2024

June 28, 2024

Distribution:

Audit Committee
Dorothy Bailey
Mitra Pedoeem
Erin White
Benjamin Williams

Maryland-National Capital Park and Planning Commission
Joe Bistany
Debra Borden
James Cannistra
Mazen Chilet
Gavin Cohen
Artie Harris
Vince Hu
Len Pettiford
Peter Shapiro
Bill Spencer

Office of the Inspector General
Renee Kenney
Modupe Ogunduyile
Irith Dror

eDiscovery Audit
Table of Contents

I. EXECUTIVE SUMMARY

II. DETAILED COMMENTARY AND RECOMMENDATIONS

I. EXECUTIVE SUMMARY

A. Overall Perspective

The Maryland-National Capital Park and Planning Commission (Commission) is a bi-county agency serving Prince George's and Montgomery counties in Maryland. The Commission's staff includes career employees such as planners, park and recreation administrators, park police and administration staff. The Commission's organizational functions are conducted by several administrative departments within Central Administrative Services. These include the Office of the General Counsel (OGC) and the Office of the Chief Information Officer (OCIO).

OGC is required to retrieve evidence from electronically stored information (ESI), a process known as eDiscovery. The traditional discovery process is standard during litigation, but eDiscovery is specific to digital evidence. The evidence from electronic discovery could include data from email accounts, instant messages, social profiles, online documents, databases, internal applications, digital images, website content and any other electronic information that could be used during civil and criminal litigation.

In order to be able to find the required digital evidence, those items need to have been preserved and stored per the Commission's Records Retention and Disposal Schedule. This preservation is referred to as litigation (or legal) hold. By issuing a litigation hold, organizations notify custodians of their duty not to delete electronically stored information potentially relevant to a case. At the Commission, the OGC is responsible for issuing and enforcing the litigation holds, while the OCIO is responsible for the electronic storage and retrieval processes, including administration, backups, logs, and access security.

In 2015, the Commission implemented the process of placing employee mailboxes on litigation hold, to prevent users from permanently deleting all or chosen content. While completing a 2019 fraud, waste, and abuse investigation, the Office of the Inspector General (OIG) determined that a certain number of Microsoft Office 365 (O365) Outlook and Exchange employee mailboxes had been incorrectly removed from litigation hold.

As a result of the 2019 investigation, the OIG conducted an audit of Litigation Hold (CW-005-2020). For purposes of that audit, litigation hold was defined as a function of the eDiscovery feature in Exchange Online - Microsoft's product for managing emails and calendars.

The audit report included several major audit concerns related to formal practices and procedures for marking users' mailboxes for litigation hold; retaining and monitoring of audit logs for litigation hold marking/unmarking; and the large numbers of Exchange and Global O365 administrators with privileged access.

During audit follow-ups in 2021 and 2022, meetings were held with the OCIO and OGC to review the status of the agreed upon remediation actions. As of May 5, 2022, the audit recommendations were partially resolved. In an effort to provide the OCIO time to implement a Security Information and Event Management (SIEM) solution, the OIG decided to close the 2020 audit, and perform a new audit in Fiscal Year (FY) 2023, which was then postponed to FY 2024.

During the period between the audit and the follow-ups, the OCIO implemented the Barracuda Cloud Backup and Archiving solutions (Barracuda) for O365, which included a resolution of the remediation steps:

- developed and distributed a Barracuda Cloud Backup policy for O365 Governance[1];
- implemented backup of all logs generated from O365; and
- reduced the number of O365 administrators.

Since June 2021, Commission email that must be obtained due to a legal case are preserved forever and can now be accessed in Barracuda, eliminating the need to rely solely on O365 archived emails.

[1] M-NCPPC O365 Barracuda Backup/Restore + e-Discovery Operations Manual issued January 21, 2021; M-NCPPC Barracuda Cloud Backup for O365 Governance Manual issued January 21, 2021

B. Audit Objective, Scope, and Methodology

Audit Objective
The objective of this audit was to assess the access and security processes and procedures related to the use of Barracuda for retrieving emails and additional O365 items, and to ensure that any risks are recognized and mitigated and to assess the Commission's processes controlling and monitoring of electronically stored information, specifically emails, that are earmarked for litigation hold.

Scope
The scope of our audit included, but was not limited to, the following audit procedures:

- Interviewed OCIO personnel responsible for the administration and security of Barracuda usage and data.
- Reviewed existing policies, process, and procedures related to the Barracuda solution.
- Obtained and analyzed assignments of privileged roles in the Barracuda system.
- Performed internal analysis of logs and scripts relating to Barracuda.
- Interviewed information technology (IT) staff within Commission departments regarding their use of O365 and Barracuda for eDiscovery.

In addition, the audit scope was designed to identify possible fraud, waste, or abuse within the process(es) being audited.

Scope Limitation
The eDiscovery review only covered O365, it did not assess social media applications such as Facebook, LinkedIn, Snapchat, etc.

Methodology
During the audit, inquiry, observation, and analysis were performed. The auditor-in-charge conducted interviews of IT management and security staff at the OCIO and within the Commission departments, reviewed Barracuda related policies and practices, access and security procedures, and the use of the O365 eDiscovery feature.

This audit was conducted 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 objective.

The audit covered the period from January 1, 2021, through June 11, 2024.

Risk Analysis
Each year, the OIG submits a risk-based audit plan to the Audit Committee for approval. Units and/or processes identified for audit typically include business as well as IT areas with high inherent risk factors.

On the business side, some examples are misappropriation of Commission assets (e.g. cash, vehicles, equipment, etc.), inconsistent personnel practices, actual or perceived conflicts of interest, and procurement violations.

On the IT side, some examples are access violations, inappropriate privileged admin rights, lack of IT-related policies and procedures, and unmitigated cybersecurity risks.

Below are the risks and controls related to the audit objective. These risks, if not mitigated, can result in fraud, abuse, or data breaches, and the possibility of legal non-compliance, with the potential to cause considerable harm to the Commission.

Risk	Risk Area	Control Area	Control Description
Insider threats due to too many users having excessive privileges	Security	Access Controls	Access to Barracuda is assigned to privileged users based upon job responsibilities.
Inability to trace unauthorized access or changes to the backed-up data due to inadequate logging process implementation	Monitoring and Notifications	Audit Logs	Barracuda logs are documented, implemented and reviewed as needed.
Delayed response to critical issues if alerting systems are not properly configured	Monitoring and Notifications	Alerts and Notifications	Barracuda alerts are configured and notify the security team when a critical issue occurs.
Delayed or inexistent response to issues due to inadequate reporting process (no reports and/or not reviewed)	Monitoring and Notifications	Reporting	Barracuda reports are configured, implemented, and reviewed.
Operational errors or inefficiencies due to outdated or unclear policies/ process/SOP documentation	Documentation and Training	Documentation	Formal processes and SOPs exist to manage the proper use of Barracuda for backing up O365 data.
Legal challenges or compliance issues if emails are not retained, contrary to policy or regulation	Compliance-Legal	Retention Policies	Emails are retained per OCIO/Legal policies.

C. Major Audit Concerns

The results of our evaluation and testing procedures indicated no major or minor audit concerns.

D. Overall Conclusions

The results of our evaluation and testing procedures indicate no major weaknesses in the design or operation of internal controls for eDiscovery of O365 mailboxes. On an overall basis, we consider the controls to be satisfactory.

We wish to express our appreciation to the Office of the Chief Information Officer management and staff, and the Commission's IT departments for the cooperation and courtesies extended during the course of our audit.

Irith Dror (Jun 28, 2024 17:45 EDT)

Irith Dror, CISA, CGEIT
Senior IT Auditor

Modupe Ogunduyile

Modupe Ogunduyile, CIG
Deputy Inspector General

Renee Kenney

Renee M. Kenney, CIG, CPA, CIA, CISA
Inspector General

June 28, 2024

Conclusion Definitions

Satisfactory	No major weaknesses were identified in the design or operation of internal control procedures.
Deficiency	A deficiency in the design or operation of an internal control procedure(s) that could adversely affect an operating unit's ability to safeguard assets, comply with laws and regulations, and ensure transactions are properly executed and recorded on a timely basis.
Significant Deficiency	A deficiency in the design or operation of an internal control procedure(s) which adversely affects an operating unit's ability to safeguard assets, comply with laws and regulations, and ensure transactions are properly executed and reported. This deficiency is less severe than a material weakness, yet important enough to merit attention by management.
Material Weakness	A deficiency in the design or operation of an internal control procedure(s) which may result in a material misstatement of the Commission's financial statements or material impact to the Commission.

II. DETAILED COMMENTARY AND RECOMMENDATIONS

None