Marks Paneth LLP
685 Third Avenue
New York, NY 10017
P 212.503.8800
F 212.370.3759
markspaneth.com

MARKS PANETH
ACCOUNTANTS & ADVISORS

Date: January 28th, 2021

To: The File of the Hugh L. Carey Battery Park City Authority

From: Marks Paneth Information Technology Audit

Technology Observations and Recommendations Resulting from the October 31, 2020 Audit

---

Marks Paneth LLP has issued a management letter under AU-C Section 265 indicating we did not observe any material weaknesses. The memo below represents our observations that are either minor in nature or represent best practices pertaining to technology. Matters in this memo are as of the date of this letter. If matters should arise between this date and the date of Marks Paneth LLP's audit report on the financial statements, we will update this memo.

Exhibit I of this memo pertains to any new findings that were identified during our work in connection with Hugh L. Carey Battery Park City Authority's (BPCA) financial statement audit for the year ended October 31, 2020. Based upon our understanding of BPCA's IT General Controls which included a review of logical security, program change control, and system recovery and availability as well as obtaining information about Cyber Security controls and practices, 1 new recommendations was presented.

Exhibit II pertains to prior year recommendations that, based on our current procedures, appear to require further attention by management. The prior year recommendation has been addressed and can be found in Exhibit III.

Exhibit III pertains to the prior year recommendation from 2018, that based upon current procedures, does not appear to require further attention by management.

It should be noted that we will review management's current year responses during Marks Paneth LLP's next audit cycle.

Table of Contents

Page

OVERVIEW

During the course of our review Marks Paneth LLP's audit team met with the following individuals:

1. Jason Rachnowitz, Director of Financial Reporting
2. Neresa Gordon, Network Security Manager

Currently, BPCA's Microsoft Windows Servers are running on versions 2012 and 2016 and workstations have been upgraded to Windows10. BPCA uses the following business applications:

1. Microsoft's Dynamics GP (Great Plains) as its accounting software which was recently upgraded.
2. Paramount's WorkPlace for project accounting and procurement which was also recently upgraded.
3. ADP's SaaS-based (Software as a Service) iPayStatements and E-TIME for payroll processing and time and attendance tracking, respectively.
4. Microsoft's SaaS-based Office 365 SharePoint application for document management.

CYBERSECURITY

We also considered BPCA's Cyber Security protections and its ability to detect and prevent unauthorized internal and external access to BPCA's network, including review of policies and procedures in place to ensure secure processes are maintained. The review of Cyber Security Protections was focused on obtaining an understanding of the risk assessment and risk mitigation practices deployed at BPCA and did not include vulnerability scanning of network and penetration testing.

As a method for review, Marks Paneth referred to the NIST Cyber Security Framework which breaks down the assessment to following categories:

- Identify: *Is there a developed organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities*
- Protect: *Are there developed and implemented appropriate safeguards to ensure delivery of critical infrastructure services*
- Detect: *Are there developed and implemented activities to identify the occurrence of a cybersecurity event*
- Respond: *Are there developed and implemented activities to take action regarding a detected cybersecurity event*
- Recover: *Is there developed and implemented activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event*

Identify:

Organizational Cyber Security Policy is established and communicated throughout the organization with the intent to meet organizational goals which identify, measure, and control risk to BPCA's information systems.

BPCA utilizes an inventorying system to record and maintain IT assets so that it can properly manage and address both security risk as well as for provisioning in the event that disaster recovery is activated. This practice enables BPCA to be able to consistently apply security controls across the organization for existing and newly acquired IT equipment.

Protect: (Identify Access Management, Authentication and Access Control)

BPCA has processes in place for how Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes to govern access control so that users may be granted access to information systems that commensurate with their job responsibilities.

As defined in the MIS handbook and corroborated through interviews, the process to provision and deprovision users is initiated by Human Resources in the ticketing system. Network and application access are assigned once proper approvals are obtained. Within Great Plains, there are audit trails that exist to evidence any changes to the status of a user. Only a quarterly basis, recertification of accounts is performed by reconciling to active Human Resource employee listings. There are also policies and procedures around the access of the "Administrator" accounts on the system. Lastly there are policies and procedures for how termination of both MIS and non-MIS users is to be addressed.

The MIS handbook defines policy and procedure around Password Management for both users and "power" users of the system.

There are session management controls in place to mitigate risk of unauthorized access to an unattended terminal or workstation.

Detect:

There are various detection tools in place to monitor for and detect any unusual security patterns, events, and anomalies supporting the 200 Liberty Street office. Additionally, all other BPCA location networks have been adequately upgraded.

The following tools are currently utilized:

- Verizon manages BPCA's network, including addressing and monitoring firewalls and internet traffic;
- CISCO network switch to isolate network traffic to data and voice VLAN for all computers and phones at BPCA office;
- Fortinet and SonicWall firewalls limit the network traffic to and from the computers at BPCA office and the Internet;
- Symantec Endpoint Protection malware and antivirus software;
- Spam filters to log and evaluate any unusual patterns;
- Monthly vulnerability scans;
- Cyber Awareness training through phishing and spoofing tests to end users; and
- BYOD protection with the VMware's AirWatch Mobile Device Management (MDM) platform, which includes the ability to delete ("wipe") data on the mobile devices.

On an annual basis, there is Cyber Training embedded within required employee training.

Respond:

Verizon monitors the activity on the BPCA network and as such would be responsible to invoke Incident Response Procedures should unusual activity be detected. There are defined policies and procedures for communication and notification to BPCA.

Recover:

Defined backup and restore procedures as well as a formal and tested Disaster Recovery Plan exists for BPCA.

Cyber Insurance:

We were also informed that BPCA has purchased cyber insurance to mitigate losses from a variety of potential cyber incidents, including data breaches, business interruption, and network damage. As a best practice, we recommend that BPCA's Audit Committee, Legal or other appropriate Board Committee members, review the summary of policy provisions to confirm coverage and ensure all necessary precautions for BPCA's business is addressed.

Hugh L. Carey Battery Park City Authority

Technology Observations and Recommendations Resulting from October 31, 2020 Financial Audit

Exhibit I – Current Year Recommendations

Observation 1 (FY20): We noted that a formalized and approved Disaster Recovery Plan exists, however associated testing was not conducted in FY20.

Recommendation: To work toward a more resilient environment, we recommend that management reaffirm their Disaster Recovery/Business Continuity plan to enable business processes to operate manually and uninterrupted in the event of unforeseen circumstances. Furthermore, we recommend the Disaster Recovery plan be tested at least annually to ensure that, in the event of an emergency, the plan is effective. Being prepared in the event of a breach is the best defensive action an Organization can take to minimize the risk posed by a potential cyber security attack.

Management's FY20 Response: *Due to the pandemic this was not completed for FY20. We will accomplish in FY21.*

Exhibit II – Prior Year Recommendations Requiring Further Action

Prior Year Recommendations Remediated

Exhibit III – Prior Year Recommendations That Do Not Appear to Require Further Action

1. *Outdated Firewall Device*