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

MARKS PANETH
ACCOUNTANTS & ADVISORS

October 21, 2019

To the Members of the Joint Audit Committee of the
New York City Municipal Water Finance Authority and
New York City Water Board

In planning and performing our audit of the combining financial statements of the New York City Municipal Water Finance Authority and the New York City Water Board, which collectively comprise the New York City Water and Sewer System (the "System"), a component unit of The City of New York, as of and for the year ended June 30, 2019, in accordance with auditing standards generally accepted in the United States of America, we considered the System's internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the combining financial statements, but not for the purpose of expressing an opinion on the effectiveness of the System's internal control. Accordingly, we do not express an opinion on the effectiveness of the System's internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency or combination of deficiencies in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis.

Our consideration of internal control was for the limited purpose described in the first paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. However, material weaknesses may exist that have not been identified.

In addition, we made recommendations and suggestions, which, if implemented, could further strengthen the internal controls and business practices (see attached Exhibits). The System's responses to our observations and recommendations were not subjected to any auditing procedures and, accordingly, we express no opinion on the responses.

This report is intended solely for the information and use of the Board of Directors, Joint Audit Committee and management of the System and is not intended to be and should not be used by anyone other than these specified parties, unless permission is granted.

Sincerely,

Marks Paneth LLP

MARKS PANETH LLP

Morison KSi

NEW YORK CITY WATER AND SEWER SYSTEM
MANAGEMENT LETTER RECOMMENDATIONS
RESULTING FROM THE JUNE 30, 2019 AUDIT

There were no new observations and recommendations that we noted during our work in connection with the audit of the combining financial statements of the New York City Water and Sewer System (the "System") as of and for the year ended June 30, 2019. Exhibit I pertains to prior year recommendations that, based on our current procedures, appear to require further attention by management. Exhibit II are those observations and recommendations from the prior year's letter that appear not to require further action.

The System is a joint operation consisting of two legally separate and independent entities, the New York City Municipal Water Finance Authority (the "Authority") and the New York City Water Board (the "Water Board"). The System is a component unit of The City of New York (the "City").

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

OVERVIEW

On September 26, 2019, Marks Paneth LLP's IT audit team met with the following individuals:

1. Farhan Abdullah, Director of Service Desk
2. Dan Chin, Computer Specialist
3. Keino Leitch, Director of IT Planning and Engineering
4. Cecil McMaster, Chief Information Officer
5. Purna Movva, CIS Application Development
6. Omar Nazem, Water Board Treasurer
7. Romel Osbourne, representative of the Director of IT Planning and Engineering
8. Michael Shum, Chief of Staff for IT
9. Gary Sidoti, Computer Systems Manager
10. Charles Thompson, Director of Infrastructure
11. Eddie Wan, Applications Development
12. Jian Zhang, Information Security Officer

Our examination was performed in conjunction with the System's combining financial statement audit for the year ended June 30, 2019. We considered the internal controls within the Information Technology ("IT") infrastructure and collected and evaluated evidence of the Water Board's information systems, practices, and operations in order to 1) assist the Marks Paneth LLP audit team to gain reliance on the computer controls for an effective and efficient audit process through the validation that information systems are safeguarding assets and maintaining data integrity and 2) provide recommendations as to whether the use of automation is being optimally utilized and operating effectively and efficiently to contribute to the Water Board's goals and objectives.

The Department of Environmental Protection's ("DEP") Office of Information Technology ("OIT") provides IT infrastructure and support for the Water Board.

Through DEP, the Water Board relies on several technology systems, some provided by outside vendors, to conduct its business processes. The core systems include:

1. Customer Information System ("CIS") initially developed by [redacted] and currently hosted by the [redacted] and developed and maintained by OIT.
2. Hardware and software provided and maintained by [redacted] for the transmission of consumption data from water meters to a central database.
3. [redacted] to manage and maintain the wireless infrastructure for the transmission of consumption data and host the servers which house the central database, [redacted] for lockbox and other payment processing services for receipt of customer payments.

5. [redacted] which handles printing, handling and mailing of sewer invoices for City and upstate customers.
6. The Water Board is also working with [redacted] to help with the design and implementation of the new [redacted] system, which will be replacing the mainframe-based CIS system.

The following observations and recommendations are focused on:

1. Outdated Server Operating System
2. Account Review and Recertification
3. Application Administrator Password Management
4. Network Administrator Password Management
5. Business Continuity and Disaster Recovery Planning

CYBER SECURITY

We also considered the Water Board's Cyber Security protections and its ability to detect and prevent unauthorized internal and external access to the network, including review of policies and procedures in place to ensure secure processes are maintained. This was a cursory review of the Water Board's Cyber Security program and did not include things such as 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: *Are 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 Water Board with the intent to meet organizational goals which identify, measure, and control risk to the Water Board's information systems.

Physical Devices within the Water Board are maintained in inventory. The inventory listing details the following components:

1. Asset Name
2. OS Version
3. Procurement information including Service Warranty dates

This practice of inventorying all information systems on the network reduces the risk that appropriate and adequate security controls may not be applied to the complete scope of the Water Board information systems.

There is a mechanism in place whereby asset vulnerabilities are identified and documented so that vulnerabilities can be prioritized and remediated in a controlled manner to reduce the risk of a system compromise.

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

The Water Board 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.

Additionally, the Water Board has deployed a formal Password Policy which leverages unique usernames and passwords (i.e. identities) for user to ensure appropriate access and the ability to track interactions between users and systems. This policy also addresses password length requirements, complexity requirements and password duration/reset.

There are policies in place for the periodic audit by the Water Board of both the network and application access accounts and recertification of permissions assigned to the accounts.

Policies exist to control access to systems remotely. Access requires the use of VPN with Multi-Factor Authentication which thereby reduces the risk of access and compromise of information systems.

A mobile device policy exists and is communicated to all employees who are issued a phone or tablet. Employees must sign a contract stating they understand the expectations for usage of a DEP issued device. The Water Board does not allow for Bring Your Own Device "BYOD" to employees.

The DEP Bureau of Business Information Technology ("BIT") sends out a monthly cyber security newsletter (the last Thursday of the month) and monthly cyber security training video (last week of the month) to all DEP users.

Detect:

There are various detection tools in place to monitor for and detect any unusual security patterns, events, and anomalies. There are controls in place over the perimeter and network security including firewalls, IDS and vulnerability assessments

Specifically, the following the monitoring tools are in place:

- [redacted]
- [redacted]
- Anti-Virus protection
- Email Spam Filtering

Additionally, penetration testing of the web application is currently being performed. Some issues were identified and immediately corrected. As the penetration test continues, any critical issues that may identified will be remediated.

Respond:

The Water Board has an Incident Response Plan in place to handle the response to a data breach in accordance with contractual, statutory, and/or regulatory obligations. The Security Team have classified incidents into different categories for how they address the issue. They maintain details regarding the system impact, software that may have been compromised, performance issues, access level issues.

Additionally, should a new threat be introduced, Patch Management procedures are in place for "patching" all critical applications immediately. Further, monthly server patching is scheduled.

Recover:

See Detailed Report finding regarding Disaster Recovery.

We would recommend that as part of DR Planning, various scenarios (e.g. malware, ransomware) be addressed and tested.

Cyber Insurance:

We were informed that the Water Board follows the lead of the City and self-insures against cyber related threats.

EXHIBIT I – PRIOR YEAR OBSERVATIONS REQUIRING FURTHER ATTENTION

1. Outdated Server Operating System (Prior Year Observation #1)

Observation (FY 2017): We were informed that the DEP has two (2) servers running the [redacted] operating system and 115 servers running [redacted] operating system. All support from Microsoft for [redacted] and [redacted] ended entirely on July 13, 2010, and July 14, 2015, respectively

Initial Recommendation: Management should consider allocating the necessary resources to ensure that all of the servers provided to the Water Board by the DEP are running an operating system which is covered by Microsoft Mainstream Support. The continued operation of unsupported operating systems poses a serious cybersecurity risk to the organization. For example, Microsoft has issued security warnings about continuing to run [redacted] after July 2015, releasing this statement: "*We have found in our research that the effectiveness of antimalware solutions on out-of-support operating systems is limited. Given the fast pace of technology, it has become increasingly important that customers use modern software and hardware that is designed to help protect PCs and servers against today's threat landscape.*"
[redacted]

FY 2018 Status: We were informed that the Water Board is still in the process of upgrading all the 117 outdated servers running either the [redacted] or the [redacted] to versions of Microsoft server which are actively supported by the software manufacturer, as well as migrating some of activities/functions currently performed by these servers to Microsoft's SaaS-based (Software as a Service) Office 365 services. We continue to recommend that management consider allocating the resources necessary to ensure that all of the organization's servers to running operating systems which are covered by Microsoft Mainstream Support.

Management's FY 2018 Response: We agree and will continue the decommissioning of [redacted].

FY 2019 Marks Paneth Status Update: During our meeting on 9/26, we were informed that IT is continuing to upgrade outdated servers running [redacted] Operating systems. Our review of the inventory list presented that there are approximately 17 servers that are still on [redacted]. It is our understanding from our discussions with IT that these servers do not maintain financial system related data.

We continue to recommend that these remaining servers be migrated to more current operating systems to ensure seamless support from Microsoft.

Management's FY 2019 Response: Management accepts the recommendation and continues to work toward the decommissioning of the remaining [redacted] and [redacted] servers.

2. Account Review and Recertification (Prior Year Observation #2)

Observation (FY 2016): We were informed DEP OIT performs a formal review of the active and inactive CIS access accounts and also recertifies the permissions associated with the active accounts. DEP OIT performs an informal review of active and inactive network access accounts; however, it does not recertify permissions associated with the active network accounts.

Initial Recommendation: DEP OIT should consider creating written policies and implementing procedures for the internal review and recertification of network access accounts which should include, at a minimum:

Network accounts: A process owner other than IT should be identified to manage the audit of network access accounts. We suggest the network account review and recertification be performed quarterly and include, at a minimum:

1. A review of active network accounts against the list of staff, temps, contractors, and consultants who have been approved for access; disable or purge all accounts that should not have access
2. A recertification of the permissions assigned to all active accounts, making sure that all accounts have the proper and appropriate privileges (e.g. read/write permissions)
3. A review of the security and or access change logs for DEP OIT systems to determine whether any temporary or "ghost" accounts have been created since the previous audit and identify unusual or anomalous activity such as:
    a. Access during non-business hours
    b. Unusual patterns of access activity
    c. Access to perform activities outside the normal scope of the user's duties

FY 2018 Status: We were informed that the Water Board is in the process of writing policies and implementing procedures mandating that network access accounts are audited on a scheduled, periodic basis. We continue to recommend that management allocates the resources necessary to write policies and implement procedures governing the internal review and recertification of network access accounts.

Management's FY 2018 Response: We agree and will develop policies and implement procedures to govern the internal review and recertification of network access accounts.

FY 2019 Marks Paneth Status Update: This appears to remain an observation. Policies and procedures were not presented to us for review that a process to review network access accounts on a regular basis is being performed. We would continue to recommend that policies and procedures are defined for the review and recertification for network accounts.

Management's FY 2019 Response: Management agrees with the recommendation and continues to develop policies and implement procedures to govern the internal review and recertification of network access accounts.

3. Network Administrator Password Management (Prior Year Observation #4)

Observation (FY 2016): We were informed that DEP OIT does not have written policies and procedures for the recording and storage of Administrator passwords for the network and network devices in a centralized, encrypted storage area, as relates to areas such as domain and enterprise administration, firewalls, routers, switches, backup storage, and cloud systems.

Initial Recommendation: DEP OIT should consider creating written policies and implementing procedures to maintain a full list of all Administrator passwords. The procedure should address:

1. How to store the lists (e.g. paper, digital): If a list is printed out, it should be stored in a sealed envelope in a fire-rated safe. Digital copies should be encrypted, using at minimum a 512-bit encryption key.
2. What should be stored on the list, such as the Administrator passwords for the network, critical network devices (e.g. firewalls, routers), encryption keys, and Internet records information (e.g. domain name registrar(s), MX record holder, and contact information).

3. Who in executive management should know how to access the lists in an emergency. Access to the list should be consistent with roles and responsibilities.
4. Where to store the lists: At a minimum, one copy should be stored onsite, and a second copy stored offsite, so passwords are available in the event the main office is inaccessible
5. Instructions how to access the lists: A member of executive management should know the procedures to access the lists in an emergency.
6. "Break glass" procedures to ensure formal notification when executive management accesses the lists.
7. Requirements to keep the lists up to date.

FY 2018 Status: We were informed that the Water Board is in the process of implementing [redacted] password management solution. We continue to recommend that management allocates the resources necessary to complete the implementation of [redacted] password management solution as well as write policies and implement procedures governing the control and management of the organization's administrative access account credentials.

Management's FY 2018 Response: We agree and will develop policies and implement procedures governing the control and management of the organization's administrative access account credentials.

FY 2019 Marks Paneth Status Update: During our discussion on 9/26, we were provided an update that the Water Board has initiated and completed "Phase 1" of the [redacted] password management tool. This solution will be an enabler to manage the process. To complement this, we continue to recommend that procedures be documented and formalized to govern the control of privileged/administrative accounts at the network level.

Management's FY 2019 Response: Management accepts this recommendation and continues to work toward full formalization of procedures and documentation governing the control of network accounts.

4. Business Continuity and Disaster Recovery Planning (Prior Year Observation #5)

Observation (FY 2016): We were informed that DEP OIT employs business continuity procedures. However, DEP OIT does not have a written Business Continuity and Disaster Recovery Plan. We were informed a Plan is in development.

1. The CIS is hosted by [redacted] which provides data and server backups and disaster recovery capabilities
2. [redacted] will provide business continuity workstations at its facilities in the event the DEP location is inaccessible
3. The consumption data from water meters is transmitted to two separate locations hosted by [redacted]

Initial Recommendation: DEP OIT should consider creating a written Business Continuity Plan to ensure financial and critical operational processes can be recovered as quickly as possible in the event of a severe business interruption. Our planning recommendations are for outline purposes only. It would be impractical, as part of this assessment process, to offer all the necessary components of a fully operational plan.

1. Conduct a Business Impact Analysis to determine the mission-critical functions at DEP OIT, who performs them, and what resources would be needed in a business interruption. Many of these critical functions may not be IT functions. As part of the Business Impact Analysis:

   a. Evaluate and document the Recovery Point Objective ("RPO") for each mission-critical function if applicable. *The RPO is the amount of time prior to a disruption for which the lack of data backup is acceptable.* For example, an RPO of two hours means that data lost up to two hours before a disruption will be restored by means other than a restore of a digital backup.
   b. Evaluate and document the Recovery Time Objective ("RTO") for each of the mission-critical functions identified in the Business Impact Analysis. *The RTO is the amount of time allowed for the restoration of a business process in order to avoid unacceptable consequences from a severe disruption.* Include in the evaluation "busier" times of year when determining the RTO.
2. Fully document critical functions and their corresponding procedures and include them in the Business Continuity Plan. Draft the procedures to be used by technically proficient people, but who may not have direct knowledge about DEP OIT's operations, networks, and infrastructure.
3. Ensure the Disaster Recovery Plan documents include all critical staff and vendor contact information.
4. Ensure documentation of inventories of all critical equipment in sufficient detail to guide repurchase decisions if required.
5. Determine an alternate meeting place in the event your current location becomes inaccessible, as part of an overall disaster recovery plan.
6. Document the procedure on how to migrate back to a normal production environment after the emergency situation has been resolved.
7. Include documentation of all data backup and restore procedures and periodic review that the procedures meet the RPO requirements.
8. Include a schedule of ongoing restore testing of data backups to ensure data backed up both onsite and offsite is available and not corrupted.
9. Include requirements for, at a minimum, a test of failover and failback test of all IT systems.

FY 2018 Status: We were informed that, in line with the organization's plan to upgrade its BCDR capabilities, the DEP OIT is in the process of installing a [redacted] for [redacted]. We were also informed that the Water Board is in the process of establishing a colocation facility in [redacted]. We continue to recommend that management allocates the resources necessary to ensure that the project stays on track as well as that an accompanying BCDR plan is written, so as to ensure financial and critical operational processes can be recovered as quickly as possible in the event of a severe business interruption.

Management's FY 2018 Response: Agree, we will work towards procuring a colocation facility.

FY 2019 Marks Paneth Status Update: The development of a Disaster Recovery/Business Continuity Plan is still in process. The Water Board will be using a colocation site in [redacted] which is about [redacted] out of the City which provides geographic diversity should there be a disruption to the primary site.

We continue to recommend the development of a DR/BCP plan to document how recovery will be executed in the event of a business disruption. This includes defining business recovery time and point objectives for the business, recovery procedures, communication and coordination protocols.

Additionally, testing to the colocation facility should be conducted on a regular basis to ensure the availability of data. Scenarios should also include security compromise on the system and ability to restore.

Management's FY 2019 Response: Management accepts this recommendation and intends to conduct regular testing of data available stored at the colocation facility. Management is also studying approaches to implementing a Disaster Recovery/Business Continuity Plan.

**** END OF REPEAT RECOMMENDATIONS****

EXHIBIT II – PRIOR YEAR RECOMMENDATIONS THAT APPEAR NOT TO REQUIRE FURTHER ACTION

5. Application Administrator Password Management (Prior Year Observation #5)

Observation (FY 2016): We were informed that Administrative access to the CIS is divided into [redacted] "sub-master" accounts with access to specific sections of the system, such as account management and database access; a master administrative account does not exist. While we understand that segregating duties can improve security, our concern is an emergency, full access to CIS is not available. We were also informed DEP OIT does not have formal written documentation detailing the functional scope of the [redacted] sections and who has access to each section. In addition, DEP OIT does not have written policies and procedures for the recording and storage of Administrator passwords for CIS and other financial and operational applications in a centralized, encrypted storage area.

Initial Recommendation: DEP OIT should consider creating written policies and implementing procedures to maintain full documentation of all Administrator passwords including storage of the passwords. The procedure should address:

1. Creating detailed documentation of the functional scope of the [redacted] sections of CIS and who has administrative access to each section
2. Creating a master account to CIS which has administrative access to all [redacted] sections of CIS to provided full access in an emergency; if creating a master account is not feasible, creating [redacted] separate administrator accounts to be used for emergency access only
3. Creating lists of application administrator account passwords and how to store the lists (e.g. paper, digital). If a list is printed out, it should be stored in a sealed envelope in a fire-rated safe. Digital copies should be encrypted, using at minimum a 512-bit encryption key
4. What should be stored on the list, such as the Administrator passwords for the application and the application database (back-end), licensing and registration information, and DEP OIT staff who are authorized to contact vendors
5. Who in executive management should know how to access the lists in an emergency. Access to the list should be consistent with roles and responsibilities.
6. Where to store the lists: At a minimum, one copy should be stored onsite, and a second copy stored offsite, so passwords are available in the event the main office is inaccessible
7. Instructions how to access the lists: A member of executive management should know the procedures to access the lists in an emergency
8. "Break glass" procedures to ensure formal notification when executive management accesses the lists
9. Requirements to keep the lists up to date

FY 2018 Status: We were informed that the Water Board is in the process of implementing [redacted] password management solution. We continue to recommend that management allocates the resources necessary to complete the implementation of [redacted] password management solution as well as write policies and implement procedures governing the control and management of the organization's administrative access account credentials.

Management's FY 2018 Response: We agree and will develop policies and implement procedures to govern the control and management of the organization's administrative access account credentials

FY 2019 Status Update: During our discussion on 9/26, we were provided update that the Water Board has initiated and completed "Phase 1" of the [redacted] password management tool. Procedures are also in place for maintaining the Administrative passwords. A privileged Identity and Access Management policy is in place to govern the control of privileged/administrative accounts. Hence, this observation is remediated.

**** END ****