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 25, 2018

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, 2018, 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
Independent member

NEW YORK CITY WATER AND SEWER SYSTEM
MANAGEMENT LETTER RECOMMENDATIONS
RESULTING FROM THE JUNE 30, 2018 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, 2018. 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 9, 2018, Marks Paneth LLP’s Tailored Technologies met with the following individuals:

1. Omar Nazem, Treasurer
2. Farhan Abdullah, Director of Service Desk
3. Dan Chin, Computer Specialist
4. Cecil McMaster, Chief Information Officer
5. Purna Movva, CIS Application Development
6. Romel Osbourne, representative of the Director of IT Planning and Engineering
7. Michael Shum, Chief of Staff for IT
8. Gary Sidoti, Computer Systems Manager
9. Charles Thompson, Director of Infrastructure
10. 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, 2018. 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 uses:

1. Customer Information System (“CIS”) initially developed by PricewaterhouseCoopers and currently hosted by the NYC Department of Information Technology and Telecommunications (“DoITT”) and developed and maintained by OIT.
2. Hardware and software provided and maintained by Aclara Technologies LLC for the transmission of consumption data from water meters to a central database.
3. Northrop Grumman to manage and maintain the wireless infrastructure for the transmission of consumption data and host the servers which house the central database, under the terms of a City-wide contract overseen by DoITT.
4. Citigroup Inc.’s Citibank for lockbox and other payment processing services for receipt of customer payments.

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

CYBERSECURITY

We also considered the Water Board's cybersecurity protections and its ability to detect and prevent unauthorized internal and external access to the Water Board's network. We looked at the policies and procedures in place to ensure secure processes are maintained, and Water Board staff is informed of current, secure practices. It would be impractical as part of this IT assessment process to provide a full cybersecurity review. Cybersecurity protections at the Water Board include:

	2018 Status	2017 Status
1. A Business Continuity and Disaster Recovery Plan is in place.	Needs improvement	Needs improvement
2. IT is evaluated regularly for risks and any identified risks are appropriately addressed	Meets requirements	Meets requirements
3. Controls over the perimeter and network security are in place. Such controls may include firewalls, routers, terminal service devices, wireless security, intrusion detection, and vulnerability assessments where appropriate.	Meets requirements	Meets requirements
4. Controls over the Water Meter Reading system, such as data encryption and data transmission protections	Meets requirements	Meets requirements
5. Anti-malware systems to protect against malicious software are deployed and actively updated on all servers, workstations, and computing devices.	Meets requirements	Meets requirements
6. Spam filtering is deployed and actively updated to block unwanted commercial emails and malicious attachments	Meets requirements	Meets requirements
7. A backup and data retention policy/schedule exists; application data and file server backups are performed to minimize the risk of lost or corrupted data; backup tapes or other media are secure (accessible only by authorized personnel); and a copy of backed up data is stored in a secure off-site location	Meets requirements	Meets requirements
8. Formal test restores of backed up data -- files and databases -- is performed periodically.	Meets requirements	Meets requirements
9. A formal password policy is distributed to all staff and procedures exist and are followed to maintain the effectiveness of authentication and access mechanisms (e.g., password length, password history, password expiration, and lockout for failed attempts).	Meets requirements	Meets requirements
10. Procedures exist and are followed to ensure timely action relating to requesting, establishing, issuing, suspending, modifying, and closing user accounts, including appropriate authorization; and user access rights are removed or suspended in a timely manner when employees are terminated	Meets requirements	Meets requirements

11. User access rights (network, application, and database) are granted on a need-to-know, need-to-do basis that considers appropriate segregation of duties and controls are in place to ensure that all users are identified uniquely	Meets requirements	Meets requirements
12. Network access accounts are periodically reviewed for access rights and permissions by non-IT management	Needs improvement	Needs improvement
13. Application data owners perform a periodic review of user access rights and permissions for all in-scope applications.	Meets requirements	Meets requirements
14. Internet content filtering is deployed either as an additional firewall module or dedicated appliance/service	Meets requirements	Meets requirements
15. Penetration testing is performed by an independent third party to analyze risks from outsiders accessing the network (external testing) and the security configurations on the network (internal testing)	Meets requirements	Meets requirements
16. Formal remote access policies and procedures for staff and third-parties are in place and enforced	Meets requirements	Meets requirements
17. BYOD protection is provided by a mobile device management platform, which includes the ability to delete ("wipe") data on the mobile devices.	Meets requirements	Meets requirements
18. Current PCI compliance certification has been obtained by the organization and or external vendors as required	Not applicable	Not applicable

EXHIBIT I – PRIOR YEAR OBSERVATIONS REQUIRING FURTHER ATTENTION

1. Outdated Server Operating System (Prior Year Observation #2)

Observation (FY 2017): We were informed that the DEP has two (2) servers running the Windows 2000 operating system and 115 servers running Windows Server 2003 operating system. All support from Microsoft for Windows 2000 and Windows Server 2003 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 Windows Server 2003 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.*"
(https://blogs.technet.microsoft.com/enterprisemobility/2015/01/23/system-center-endpoint-protection-support-for-windows-server-2003/)

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 Windows 2000 or the Windows Server 2003 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 Windows 2000 and Windows 2003 servers.

2. Account Review and Recertification (Prior Year Observation #4)

Observation (FY 2016): We were informed DEP OIT performs a formal review of the active and inactive Customer Information System ("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:

<u>Network accounts</u>: 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.

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

Observation (FY 2016): We were informed that Administrative access to the CIS is divided into five "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 five 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 five sections of CIS and who has administrative access to each section
2. Creating a master account to CIS which has administrative access to all five sections of CIS to provided full access in an emergency; if creating a master account is not feasible, creating five 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 Bomgar's password management solution. We continue to recommend that management allocates the resources necessary to complete the implementation of Bomgar's password management solution as well as write policies and implement procedures governing the control and management of the organization's administrative access account credentials (please refer to the *"Network Administrator Password Management (Prior Year Observation #6)"* section for further details).

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

4. Network Administrator Password Management (Prior Year Observation #6)

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 Water Board is in the process of implementing Bomgar’s password management solution. We continue to recommend that management allocates the resources necessary to complete the implementation of Bomgar’s password management solution as well as write policies and implement procedures governing the control and management of the organization’s administrative access account credentials (please refer to the *“Application Administrator Password Management (Prior Year Observation #5)”* section for further details).

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.

5. Business Continuity and Disaster Recovery Planning (Prior Year Observation #7)

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 DoITT which provides data and server backups and disaster recovery capabilities
2. DoITT 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 Northrop Grumman

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 Hitachi Unified Compute Platform ("UCP") for VMware vSphere. We were also informed that Water Board is in the process of establishing a colocation facility in Hawthorne, New York. 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.

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

<u>EXHIBIT II – PRIOR YEAR RECOMMENDATIONS THAT APPEAR NOT TO REQUIRE FURTHER ACTION</u>

6. Management Steering Committee (Prior Year Observation #1)

7. Cyber Insurance (Prior Year Observation #3)

**** END ****