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

New York
New Jersey
Pennsylvania
Washington, DC

MARKS PANETH
ACCOUNTANTS & ADVISORS

December 1, 2016

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, 2016, 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 Schedule). The Authority’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

NEW YORK CITY WATER AND SEWER SYSTEM
MANAGEMENT LETTER RECOMMENDATIONS
RESULTING FROM THE JUNE 30, 2016 AUDIT

Exhibit I below lists new items that we noted during our 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, 2016. 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").

OVERVIEW

On October 7, 2016, Marks Paneth's Tailored Technologies met with the following Department of Environmental Protection ("DEP") employees: Omar Nazem, Treasurer, Charles Thompson, Director of Infrastructure, Keino Leitch, Director of IT Planning and Engineering, Farhan Abdullah, Director of Service Desk, Purna Movva, CIS Application Development, and Gary Sidoti, Computer Systems Manager. Our procedures were performed in conjunction with the System's combining financial statement audit for the year ended June 30, 2016. 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 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 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 DEP's 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.

We also considered the Water Board's cyber security protections and its ability to detect and prevent unauthorized internal and external access to the City's network and the DEP Water Meter Reading system. We looked at the policies and procedures in place to ensure secure processes are maintained, and DEP staff is informed of current, secure practices. It would be impractical as part of this IT audit process to offer a full cyber security review.

The following observations and recommendations are focused on the need to:

1. Improve review and recertification of network access accounts
2. Improve management of application and network administrator passwords
3. Improve remote support permissions
4. Improve Business Continuity and Disaster Recovery documentation

EXHIBIT I – CURRENT YEAR RECOMMENDATIONS

1) ACCOUNT REVIEW AND RECERTIFICATION

Observation: 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.

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 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 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
    a. Access to perform activities outside the normal scope of the user's duties

Management's Response: DEP OIT will review the recommendation against current policies and procedures and determine whether to implement the recommendation. DEP OIT and the Bureau of Customer Service currently follow the procedures stated in the "CIS Authorization" memo dated June 30, 2015. Given the low rates of staff turnover, and resulting long average tenures seen within DEP's workforce, it is not necessary to recertify certain classes of passwords and access privileges as often as may be the case in other types of organization. In addition, users can only make changes to CIS data while logged into the system, which provides an audit trail and acts as a deterrence against misuse. The CIS system is also used to periodically run screens against account data to detect irregular account activity.

2) APPLICATION ADMINISTRATOR PASSWORD MANAGEMENT

Observation: We were informed that Administrative access to the CIS system 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.

Recommendation: DEP OIT should consider creating written policies and implementing a 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

Management’s Response: DEP OIT will review the recommendation against current policies and procedures and determine whether to implement the recommendation. DEP OIT currently followings the procedures stated in (1) the CIS recertification email dated November 23, 2015 and (2) the CIS password policy email dated July 1, 2015. All administrator password procedures are routinely reviewed against the list of employees involved and their responsibilities, and DEP OIT believes that appropriate checks and redundancies are in place. DEP OIT will determine whether it is possible to further enhance existing policies. In the past, DEP OIT has assessed the idea of a master administrator account, and determined that the security benefits of not having such an account outweigh the convenience that such an account would provide in an emergency situation, and that this tradeoff can be made without introducing significant financial or operational risk to DEP.

3) NETWORK ADMINISTRATOR PASSWORD MANAGEMENT

Observation: 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.

Recommendation: DEP OIT should consider creating written policies and implementing a 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 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

Management’s Response: DEP OIT will review the recommendation against current policies and procedures and determine whether to implement the recommendation. All administrator password procedures are routinely reviewed with the employees involved, and DEP OIT believes that appropriate checks and redundancies are in place. DEP OIT will determine whether it is possible to further enhance existing policies. In the past, DEP OIT has assessed the idea of a centralizing administrator account access information, and determined that the security benefits of not having such centralization outweigh the convenience that would be available in an emergency situation, and that this tradeoff can be made without introducing significant financial or operational risk to DEP.

4) REMOTE SUPPORT PERMISSIONS

Observation: We were informed that OIT uses the Goverlan Remote Administration application to remotely access staff workstations to perform support functions. While Goverlan provides an alert to users that OIT staff is accessing the workstation remotely, the OIT staff is able to gain access to the computers at will. The concern is that an OIT staff member may access a computer while sensitive or confidential financial or personnel information is displayed on the screen.

Recommendation: Management should consider reviewing the procedures for OIT staff to access computers remotely. Best practices dictate that a user should actively grant permission to initiate a remote support session. While we recognize that the risk of viewing sensitive information on many of the computers which OIT accesses remotely is low, we recommend that the OIT staff configure the computers which are regularly used to access sensitive or confidential financial or personnel information to require the user to actively grant permission to initiate a remote support session.

Management's Response: DEP OIT will review the recommendation against current policies and procedures and determine whether to implement the recommendation. The use of remote access software is permissible solely for the purpose of remote desktop support via authorized persons. Remote connection privileges are only granted to authorized and trained OIT support staff. In addition, the remote technician can only establish a remote session from authenticated, single-account services, where any session can be traced to a particular technician, creating both an audit trail and a deterrent against inappropriate use of the software. Remote connections are only made in response to a recognized user's request made through normal OIT channels and the remote access software is configured to show with a visible identifier that a remote access session is taking place. DEP OIT will review the recommendation against current policies and procedures and determine whether to implement the recommendation for users with access to sensitive or confidential financial or personnel information.

5) BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

Observation: 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

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 minimum, a test of failover and failback test of all IT systems

Management's Response: DEP OIT has extensive disaster recovery policies and redundancy plans in place, and all DEP OIT employees have received the applicable training concerning these policies and plans. A comprehensive review of DEP policies and procedures was conducted following Hurricane Sandy, and many policies and procedures were updated at that time. DEP OIT currently has a project underway to assess the best path to take in assembling existing policies and plans into a single comprehensive Business Continuity and Disaster Plan.

**** END ****