

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

New York
New Jersey
Pennsylvania
Washington, DC
Florida

M A R K S P A N E T H
ACCOUNTANTS & ADVISORS

November 17, 2017

The Audit Advisory Committee and the Board of Trustees of the
New York City School Construction Authority

In planning and performing our audit of the financial statements of New York City School Construction Authority (the "Authority" or "SCA"), a component unit of The City of New York, as of and for the year ended June 30, 2017, in accordance with auditing standards generally accepted in the United States of America, we considered the Authority's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Authority's internal control. Accordingly, we do not express an opinion on the effectiveness of the Authority'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 a 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 Schedules). 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 Authority's Audit Advisory Committee, Board of Trustees, management, others within the organization, and is not intended to be, and should not be, used by anyone other than these specified parties.

Sincerely,



MARKS PANETH LLP

**NEW YORK CITY SCHOOL CONSTRUCTION AUTHORITY
MANAGEMENT LETTER RECOMMENDATIONS
RESULTING FROM THE JUNE 30, 2017 AUDIT**

SCHEDULE 1 – FINANCIAL STATEMENT AUDIT OBSERVATIONS AND RECOMMENDATIONS

OVERVIEW

Included in Exhibit I is a new observation and recommendation that we noted during our audit of the Authority's June 30, 2017 financial statements. Exhibit II of this memo lists the status of our recommendations from previous years that still require management's attention. Exhibit III of this memo lists the recommendation from previous years that appears not to require further attention.

In addition, we considered the internal controls within the information technology infrastructure and collected and evaluated evidence of the Authority's information systems, practices, and operations. The observations and recommendations related to information technology are located in Schedule II.

EXHIBIT I – CURRENT YEAR NEW OBSERVATION AND RECOMMENDATION

1. REVIEW AND APPROVAL OF CREDIT CARD TRANSACTIONS

Observation: During our audit of the corporate credit card expenses, we noted there is no process in place for periodic independent review of the President's credit card charges.

Recommendation: We recommend as best practice to have the Authority's Audit Advisory Committee to designate a person to perform periodic review.

Management's Response: Management agrees with this recommendation. Though immaterial, the Authority will request the Audit Advisory Committee to designate an individual to perform a periodic review of the President's credit card statement.

**** END OF CURRENT YEAR NEW OBSERVATION AND RECOMMENDATION ****

**NEW YORK CITY SCHOOL CONSTRUCTION AUTHORITY
MANAGEMENT LETTER RECOMMENDATIONS
RESULTING FROM THE JUNE 30, 2017 AUDIT**

Exhibit II – PRIOR YEAR RECOMMENDATIONS REQUIRING FURTHER ATTENTION

2. LONG OUTSTANDING RETAINAGE PAYABLE (Prior Year Observation #2)

2015 Observation: During our audit of the retainage payable account, which reflects payments withheld from contractors until certain contract completion criteria have been met, we noted certain outstanding retainage payable that had been withheld dating back as far as 1990. Total retainage payable older than 10 years amounted to approximately \$6.6 million as of June 30, 2015.

2015 Recommendation: We recommend the Authority review the retainage payable account at least annually to determine the resolution of older retainage payable balances and to ensure that it is complying with any applicable escheat requirements.

Prior Year Management's Response: Management agrees with this recommendation. As part of the financial system upgrade currently underway, the Authority will review and investigate each aged balance within the retainage payable account. Based on the results of the investigation, the Authority will determine the necessary actions to take for the specific identified payable. The project is due to be completed by fiscal year end 2016. Subsequently, the Authority will design a process to monitor the retainage payable account annually.

2016 Update: This process is still being implemented by the Authority.

2016 Management's Response: The Authority has reviewed the aged balances within the retainage payable account and has identified action steps to be taken to address these aged balances. Based on the action steps taken, the Authority has written off approximately \$2.3 million of aged balances. The remainder of the aged balance pertain to contracts that may still have an active status therefore requiring further research, anticipated to be completed during fiscal year 2017. Management is working on designing a process to monitor retainage payable.

2017 Update: This process is still being implemented by the Authority.

2017 Management's Response: In fiscal year 2017, the SCA completed its analysis of the open retainage payable older than 10 years as of June 30, 2015. Based on completed analysis performed, the Authority has written off in total approximately \$5.4 million of aged balances. The Authority has developed an annual review process which takes into consideration status of the project and transaction history in the assessment of the retainage payable. The process will be implemented during fiscal year 2018 to review current outstanding retainage payable balances.

3. ANALYSIS OF CONSTRUCTION IN PROGRESS (Prior Year Observation #3)

2015 Observation: During our audit of construction in progress, we noted construction in progress and completed contracts are tracked as cumulative, multi-year balances on the general ledger, which are then netted to arrive at the construction in progress amount recorded as an asset at June 30th. Accordingly, the Authority was unable to readily provide a report of construction costs that comprise the open construction in progress balance at June 30th and identify those costs with individual projects. While we obtained an analysis showing that the majority (approximately 98%) of the beginning construction in progress balance as of June 30, 2014 related to projects that were completed and transferred to the Department of Education during fiscal year 2015, without a detailed analysis of the remaining construction in progress balance, there is a risk that there are amounts reflected in construction in progress that should also have been transferred to the Department of Education as part of a completed project.

**NEW YORK CITY SCHOOL CONSTRUCTION AUTHORITY
MANAGEMENT LETTER RECOMMENDATIONS
RESULTING FROM THE JUNE 30, 2017 AUDIT**

2015 Recommendation: We recommend the Authority annually prepare a detailed report of construction in progress as of June 30th on a project by project basis and review that report to ensure that there are no construction in progress costs that relate to project costs that should have been transferred to the Department of Education.

2015 Management's Response: Management agrees with this recommendation. The Authority has a process which we undertake annually to track and generate a report, detailing by building ID, all projects completed for the current fiscal year to be transferred to the Department of Education. A cumulative report of all open projects is currently not available. The Authority is creating a program to generate this report for audit purposes for fiscal year 2016. A process will be implemented, annually, to review the report to validate that construction in progress relates to projects that are actively being constructed.

2016 Update: This process is still being implemented by the Authority.

2016 Management's Response: The Authority has generated a preliminary report of open construction in progress items not transferred. The Authority is currently vetting this report in comparison to the financial ledger which historically has been a net number. This is anticipated to be completed during fiscal year 2017.

2017 Update: This process is still being implemented by the Authority.

2017 Management's Response: The Authority has instituted a reconciliation process for current and future year construction in progress activities to be performed annually. The Authority continues to review the historical open construction in progress report to ensure complete and accurate data within the report. This analysis is anticipated to be completed during fiscal year 2018.

**** END OF PRIOR YEAR AUDIT RECOMMENDATIONS REQUIRING FURTHER ACTION ****

EXHIBIT III – PRIOR YEAR AUDIT RECOMMENDATION THAT DOES NOT REQUIRE FURTHER ACTION

4. LACK OF AUDIT COMMITTEE OVERSIGHT (Prior Year Observation #1)

**** END OF AUDIT RECOMMENDATIONS ****

**NEW YORK CITY SCHOOL CONSTRUCTION AUTHORITY
MANAGEMENT LETTER RECOMMENDATIONS
RESULTING FROM THE JUNE 30, 2017 AUDIT**

SCHEDULE II – INFORMATION TECHNOLOGY OBSERVATIONS AND RECOMMENDATIONS

OVERVIEW

Our examination was performed in conjunction with the New York City School Construction Authority's (SCA) financial statement audit for the year ended June 30, 2017. We considered the internal controls within the Information Technology (IT) infrastructure, and collected and evaluated evidence of SCA'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 SCA's goals and objectives.

Currently, SCA has 376 servers running Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2016, Solaris 11, and VMware ESX 5.5/6. SCA uses:

1. Oracle's E-Business Suite (EBS) Financials version 12.2 as their accounting software
2. Workday's online system for HR information management
3. E-Pay's online system to process payroll
4. Oracle's Primavera Contract Management (CM13) for construction management tracking
5. Frontline Data Services co-location facility in Orangeburg, NY to host disaster recovery systems
6. Corus Group LLC to provide disaster recovery support services

The following observations and recommendations are focused on:

1. Cyber Insurance
2. Laptop and Portable Device Security
3. IT Rights to Financial and Operational Systems
4. Access Account Auditing
5. Business Continuity and Disaster Recovery (BCDR) Planning

**NEW YORK CITY SCHOOL CONSTRUCTION AUTHORITY
MANAGEMENT LETTER RECOMMENDATIONS
RESULTING FROM THE JUNE 30, 2017 AUDIT**

CYBERSECURITY

We also considered SCA's cybersecurity protections and its ability to detect and prevent unauthorized internal and external access to SCA's network. We looked at the policies and procedures in place to ensure secure processes are maintained, and SCA 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 SCA include:

1. Formal procedures for the creation, modification, and termination of network and application access accounts
2. IT security policies and procedures addressing use of passwords, computers, and network resources including remote access to the network
3. Data security policies addressing information privacy and security, data integrity and encryption, and information disposal
4. Data retention policies and schedules including documentation of data backup procedures which support the data retention policy
5. A combination of Checkpoint and Cisco firewall device
6. Ironport's cloud service is used to filter spam
7. Symantec's Endpoint Protection is used to defend against malware attacks on servers and workstations
8. FireEye intrusion detection and prevention appliances monitor internal and external network connections
9. Mobile device protection is provided by VMware's AirWatch mobile device management system, which includes the ability to delete ("wipe") data on the mobile devices issued by SCA. SCA does not allow employees to use their own personal devices to connect to SCA's email services and network/other information assets

**NEW YORK CITY SCHOOL CONSTRUCTION AUTHORITY
MANAGEMENT LETTER RECOMMENDATIONS
RESULTING FROM THE JUNE 30, 2017 AUDIT**

EXHIBIT I – CURRENT YEAR NEW IT OBSERVATION AND RECOMMENDATION

1. CYBER INSURANCE

Observation: We were informed that SCA has not purchased cyber insurance. Cyber insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruptions, and network damage.

Recommendation: Management should consider creating a risk profile in order to determine SCA's need for cyber insurance. Management should consider working with their insurance provider to provide an analysis of risk vs. cost. Cyber risk refers to *any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cyber-attacks, fraud committed by misuse of data, any liability arising from data storage and the availability, integrity and confidentiality of electronic information – be it related to individuals, companies or governments*¹.

The benefits of cyber insurance include, but are not limited to, the following:

1. Insurance places a dollar value on an organization's cyber risk.
2. The underwriting process can help organizations identify cybersecurity gaps and opportunities for improvement.
3. Many cyber insurance policies bring supplemental value through the inclusion of risk mitigation tools as well as significant incident response assistance following a cyber incident.

Management's Response: Management agrees with this recommendation and will evaluate the need for cyber insurance coverage.

**** END OF CURRENT YEAR NEW IT OBSERVATION AND RECOMMENDATION ****

¹ American Banker's Associate (ABA):
(http://www.aba.com/Tools/Function/Documents/2016Cyber-Insurance-Buying-Guide_FINAL.pdf)

**NEW YORK CITY SCHOOL CONSTRUCTION AUTHORITY
MANAGEMENT LETTER RECOMMENDATIONS
RESULTING FROM THE JUNE 30, 2017 AUDIT**

EXHIBIT II – PRIOR YEAR IT RECOMMENDATIONS REQUIRING FURTHER ATTENTION

2. LAPTOP AND PORTABLE DEVICE SECURITY (Prior Year IT Observation #1)

2016 Observation: We were informed SCA does not have written policies or procedures on the protection of SCA data on portable computers and storage devices. The only security installed on the SCA laptops is the standard Windows network login and password. If one of these laptops were lost or stolen, there is the potential risk the hard drive could be removed from the laptop and connected to another computer, allowing full access to potentially confidential or sensitive information. We were also informed portable USB drives are used by the staff and the data on the drives is not protected. We understand SCA will be upgrading the laptop operating system to Microsoft Windows 10 at which time laptop hard drives will be protected using the BitLocker encryption capability included with Windows 10.

2016 Recommendation: Management should consider creating a written portable computing acceptable use policy including the use of laptops, USB drives, and smart phones. At a minimum, the policy should include requirements to encrypt all SCA data stored on portable computing devices. Management should consider requiring that only portable storage devices issued by the IT Department are to be used to store SCA data.

Pending upgrades to Microsoft Windows 10, management should consider implementing data encryption software on any laptop computers and portable USB drives which might contain confidential or sensitive operational or financial information. Inexpensive data encryption software includes, but is not limited to:

- Symantec's Pretty Good Privacy (PGP)
- Check Point Full Disk Encryption
- Kaspersky's Endpoint Security Advanced

2017 Status: We were informed that SCA is in the process of implementing an acceptable use policy for the utilization of portable computing equipment and is slated to do so by the end of 2017.

We were also informed that SCA has selected Microsoft's BitLocker encryption software to encrypt all of the organization's laptops. All new SCA issued laptops are issued with BitLocker. SCA is currently working to install BitLocker on all existing/previously issued SCA laptops; SCA estimates that it has installed BitLocker on 20% of the organization's total laptops and that it will take another 6-9 months to install BitLocker on the rest of SCA's laptops. We continue to recommend that management allocate the resources necessary to ensure that BitLocker encryption software is installed on all of SCA's portable computing devices.

2017 Management's Response: SCA IT has accelerated the deployment of Microsoft Windows 10 laptops with BitLocker encryption enabled and is expected to complete deployment by the end of February 2018.

**NEW YORK CITY SCHOOL CONSTRUCTION AUTHORITY
MANAGEMENT LETTER RECOMMENDATIONS
RESULTING FROM THE JUNE 30, 2017 AUDIT**

3. IT RIGHTS TO FINANCIAL AND OPERATIONAL SYSTEMS (Prior Year IT Observation #2)

2015 Observation: Members of the SCA IT staff have administrative access to financial and critical operational applications. Within the Information Technology department, the Financial & Core Systems and the Construction, Administration & Legal Systems groups are tasked with ongoing system development and support, including the upgrade of applications. The Operations & Infrastructure group is tasked with managing all user accounts within the Oracle E-Business Suite Financials and Oracle Primavera Contract Management systems and the upgrades and maintenance to the hardware systems running the applications.

While best practices dictate removing IT staff's full administrative access to financial and critical operational systems, we understand SCA's operational efficiencies require continual administrative access for IT staff. SCA did provide us documentation detailing the authorization process for creating access accounts and procedures to set up, modify, or terminate accounts. However, the concern remains that IT staff has full access to sensitive and confidential information without full IT department compensating controls in place.

2015 Recommendation: Management should consider creating additional formal policies and implementing procedures to provide greater oversight of IT staff access to financial and critical operational applications to include:

1. The Chief Technology Officer or designated senior staff member should review access logs quarterly for each system where IT has administrative access. The review should focus on access events for IT staff with administrative privileges to 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
2. The Chief Technology Officer or designated senior staff member should review a representative sampling of user network and Oracle accounts to ensure the SCA procedures have been followed. The representative sample should include high risk accounts such as new accounts, transferred accounts, terminated accounts, and accounts with high levels of access.

2017 Status: We were informed that SCA implemented Oracle's EBS version 12.2 Application with the additional Management Pack Module which allows for privileged access account management and provides access oversight capabilities. However, after installing EBS version 12.2, SCA determined that the access account management features provided by the Management Pack Module weren't robust enough to meet the needs of the organization. As a result, SCA then began evaluating alternative tools, identifying Oracle's GRC tool.

Through discussions with Oracle representatives, SCA was informed that the latest version of Oracle's GRC application would be able to provide the access account management and oversight capabilities SCA desired. SCA was also informed, however, that Oracle had ceased offering local installations of the GRC application, only offering its cloud-based version. Thus, in order to utilize the latest version of the GRC cloud-based application, SCA was informed that it would have to also move all of its accounting and financial systems to the cloud as well. As SCA desires to keep all of the organization's data hosted locally and not in the cloud, SCA determined that the GRC application was not a viable solution.

We continue to recommend that management allocates the resources necessary to identify an alternative solution to meet the privilege access account management and oversight needs of the organization. While SCA searches for an alternative solution, for the time being, we also recommend that management allocate the resources necessary to implement additional, manual, compensating controls to provide for oversight of all IT staff access to SCA's financial and critical operational applications.

**NEW YORK CITY SCHOOL CONSTRUCTION AUTHORITY
MANAGEMENT LETTER RECOMMENDATIONS
RESULTING FROM THE JUNE 30, 2017 AUDIT**

2017 Management's Response: Management agrees with this recommendation and will establish a quarterly manual access process and procedure starting in January 2018 while continuing to identify software solutions that can satisfy this recommendation.

4. BUSINESS CONTINUITY AND DISASTER RECOVERY (BCDR) PLANNING (Prior Year IT Observation #5)

2015 Observation: We were provided with a copy of the NYCSCA Emergency Management Plan and the renewal agreement with Corus Managed Services, LLC, provider of business continuity services for SCA. Further, we were informed SCA performs an annual disaster recovery test at the Corus site. We understand the deployment of the disaster recovery site is a work in progress, however, the documentation we were provided does not include detailed action plans documenting the disaster recovery procedures. In addition, while the functionality exists for staff to connect to the disaster recover site, we were informed instructions for staff detailing how to connect to the disaster recovery servers have not been created.

2015 Recommendation: Management should consider creating formal disaster recovery action plans for the activation of the disaster recovery site at Corus. We recommend drafting the procedures to be used by people who are technically proficient but who may not have direct knowledge about SCA's operations, networks, and infrastructure. Include detailed instructions showing staff how to connect to the disaster recovery servers from workstations at SCA offices and from remote locations, such as from a home computer.

2017 Status: We were informed that SCA has completed its disaster recovery testing processes at the organization's designated warm site. We continue to recommend that management allocate the resources necessary to write a comprehensive BCDR plan so as to ensure SCA's financial and critical operational processes can be recovered as quickly as possible in the event of a severe business interruption.

2017 Management's Response: Management agrees with this recommendation. As per the internal audit performed by Ernst & Young, the Administration Department has initiated new plans and efforts to support the creation of the new BCDR plan and address any outdated information and procedures.

**NEW YORK CITY SCHOOL CONSTRUCTION AUTHORITY
MANAGEMENT LETTER RECOMMENDATIONS
RESULTING FROM THE JUNE 30, 2017 AUDIT**

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

- 5. ACCESS ACCOUNT AUDITING (Prior Year IT Observation #3)**
- 6. IT ADMINISTRATIVE PASSWORD MANAGEMENT (Prior Year IT Observation #4)**

****END OF ALL RECOMMENDATIONS****