New York City School Construction Authority

Management Letter Recommendations

(Resulting from the June 30, 2018 Audit)

November 2018

MARKS PANETH

ACCOUNTANTS & ADVISORS

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

MARKS PANETH
ACCOUNTANTS & ADVISORS

November 20, 2018

The President 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, 2018, 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 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

MARKS PANETH LLP

Morison KSi
Independent member

SCHEDULE 1 – FINANCIAL STATEMENT AUDIT OBSERVATIONS AND RECOMMENDATIONS

OVERVIEW

There were no new observations and recommendations noted during our audit of the Authority's June 30, 2018 financial statements. Included in Exhibit I is an observation and recommendation from the prior year's audit that requires further attention. Exhibit II lists the recommendations from previous years that appear 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 – PRIOR YEAR RECOMMENDATION REQUIRING FURTHER ATTENTION

1. 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 New York City Department of Education ("DoE") as part of a completed project.

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 is no construction in progress costs that relate to project costs that should have been transferred to the DoE.

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 DoE. 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. Reconciliation of the historical report to the ledger continues to be ongoing due to volume of data and information under review. The Authority is also working with the New York City Comptroller's Office to accomplish this transfer. This analysis is anticipated to be completed during fiscal year 2018.

2018 Update: During fiscal year 2018, the Authority did prepare an analysis and reconciliation of its open construction in progress to its general ledger. Based on this analysis, the Authority has identified several projects that were completed in prior years and is working with the DoE and Comptroller's Office to accomplish this transfer. It is anticipated that the construction in progress relating to several of these projects will be transferred in fiscal year 2019.

2018 Management's Response: The Authority completed an analysis of its construction in progress projects and has identified open construction in progress projects. During the performance of this analysis, the Authority identified several projects that were completed in prior fiscal years and is working with the Comptroller's Office and DoE to determine the methodology and process for transferring these projects. The transfer of these projects is anticipated to be completed in fiscal year 2019.

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

EXHIBIT II – PRIOR YEAR AUDIT RECOMMENDATIONS THAT DO NOT REQUIRE FURTHER ACTION

2. REVIEW AND APPROVAL OF PRESIDENT'S CREDIT CARD TRANSACTIONS (Prior Year Observation #1)

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

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

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, 2018. 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 SaaS-based (Software as a Service) services for HR information management
3. E-Pay's SaaS-based services for payroll processing
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. Outdated Server Operating System
2. Cyber Insurance
3. Laptop and Portable Device Security
4. IT Rights to Financial and Operational Systems
5. Business Continuity and Disaster Recovery (BCDR) Planning

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 the 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. Azure-hosted Cisco ASA and on-premise Checkpoint firewall devices deployed
6. Ironport's SaaS-based services are 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 (IDS/IPS) 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
10. Microsoft's native BitLocker software is used to encrypt laptop hard drives

Exhibit I – Current Year New Recommendations

1. Outdated Server Operating System

Observation: We were informed that four (4) of SCA's servers run the Microsoft Windows Server version 2003 operating system. All support from Microsoft for Windows Server 2003 ended entirely on July 14, 2015. These four (4) servers, however, are only turned on as-needed. Additionally, we were informed that the servers are in the process of being retired, as the legacy systems which they are hosting are in the process of being retired and are slated to be replaced by the end of FY 2019.

Recommendation: Management should consider allocating the necessary resources to ensure that all of the SCA's servers are running an operating system which is covered by Microsoft Mainstream Support. 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[1]."*

Management's Response: The system running on the server is a core application critical to the SCA. This is a multi-year effort between IT and the business operations. Retirement of servers is projected at end of 2019 calendar year.

****END OF NEW RECOMMENDATIONS****

[1] (https://blogs.technet.microsoft.com/enterprisemobility/2015/01/23/system-center-endpoint-protection-support-for-windows-server-2003/)

Exhibit II – Prior Year Observations Requiring Further Attention

2. Cyber Insurance (Prior Year Observation #1)

Observation (FY17): 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. For further information regarding cyber insurance and its benefits, a good overview is provided by the U.S. Department of Homeland Security (DHS) at the following link:
(https://www.dhs.gov/cybersecurity-insurance)

Initial 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*[2].

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.

Cyber insurance providers include, but are not limited to, the following:

1. American International Group (AIG)
(http://www.aig.com/business/insurance/cyber-insurance)
2. Chubb Limited
(https://www2.chubb.com/us-en/business-insurance/privacy-network-security.aspx)
3. XL Group Ltd.
(http://xlcatlin.com/insurance/insurance-coverage/professional-insurance/cyber-and-technology)

FY18 Status: We were informed that SCA is in the process of acquiring quotes for cyber insurance. We continue to recommend that management consider allocating the resources necessary to create a risk profile in order to determine SCA's need for cyber insurance

Management's FY18 Response: The SCA is in the process of acquiring cyber insurance quotes and completion of its risk profile.

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

3. Laptop and Portable Device Security (Prior Year Observation #2)

Observation (FY16): 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.

Initial Recommendation: Management should consider creating a written portable computing acceptable use policy including the use of laptops, USB drives, and smartphones. 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:

1. Symantec's Pretty Good Privacy (PGP) (http://www.symantec.com/business/whole-disk-encryption)
2. Check Point Full Disk Encryption (http://www.checkpoint.com/products/full-disk-encryption/index.html)

FY18 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 2018.

We were also informed that SCA has implemented Microsoft's BitLocker disk encryption software on ~95% of the organization'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.

Management's FY18 Response: Acceptable use policy for portable equipment has been drafted, pending approval and publishing of the policy. All portable devices will have BitLocker encryption installed by end of calendar year 2018.

4. IT Rights to Financial and Operational Systems (Prior Year Observation #3)

Observation (FY15): 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.

Initial 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.

FY18 Status: We were informed that SCA has continued its efforts in reaching out to vendors to source a solution which will allow for privileged access account management and provides access oversight capabilities within the Oracle EBS version 12.2 application as the local version of the application does not support such capabilities. We were also informed that SCA is about to begin a project with Splunk (i.e. with auditing enabled, Splunk logs distinct events to the audit index. Interactions with Splunk such as searches and configuration changes generate audit events) and will open discussions with them to see if they have a solution which is able to meet the organization's user access management needs within Oracle EBS. 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.

Management's FY18 Response: SCA will continue searching for alternative solution and automate the review process. While a manual check and review process was implemented in early 2018, the SCA will strengthen this process by the end of calendar year 2018.

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

Observation (FY15): We were provided with a copy of the NYCSCA Emergency Management Plan and the renewal agreement with Corus Managed Services, LLC, SCA's provider of business continuity services. 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 recovery site, we were informed instructions for staff detailing how to connect to the disaster recovery servers have not been created.

Initial Recommendation: Management should consider creating formal disaster recovery action plans for the activation of the disaster recovery site at Corus. We recommend creating 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.

FY18 Status: We were informed that SCA has completed its disaster recovery testing processes at the organization's designated warm site at Frontline Data Services in Orangeburg, NY. We were also informed that, as part of the BCDR plan, a Business Impact Analysis (BIA) has not yet been conducted. The concern is that the lack of a BIA will adversely affect recovery and, thus, the ability to perform business processes in the event of a severe business disruption. We continue to recommend that management consider allocating the resource necessary to conduct a BIA, so as to determine the critical functions at SCA, who performs them, and what resources would be needed in a business interruption; many of these may not be IT functions. As part of the BIA, the following should be performed:

1. Evaluate and document the Recovery Point Objective (RPO) for each 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
2. Evaluate and document the Recovery Time Objective (RTO) for each of the 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

Management's FY18 Response: The SCA is nearing completion of a BIA, capturing the respective RTO and RPO for all essential business processes. In addition to IT considerations, the BIA identifies essential staff, assesses interdepartmental dependencies, and forecasts potential changes over a 12-month period. Completion of the BIA is anticipated in January 2019 and will address the efficacy of the IT Disaster Recovery (ITDR)/form the foundation of a more robust Business Continuity Plan (BCP).

The BCP also will address facilities, personnel, and business processes not governed by IT systems. BCP triggering scenarios will provide clear guidelines by informing the content of recovery action plans. The BCP will align with Disaster Recovery operations and will be delivered within the first calendar quarter of 2019. Staff training on Business Continuity will commence subsequent to completion of the BCP.

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

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

There are no prior year observations and recommendations that appear not to require further attention.

****END****