Syosset Central School District

Dr. Thomas L. Rogers
Superintendent of Schools

99 Pell Lane
P.O. Box 9029
Syosset, NY 11791-9029
(516) 364-5600
Fax: (516) 921-5616

Ms. Adele Bovard
Deputy Superintendent of Schools
(516) 364-5647

Dr. Patricia M. Rufo
Asst. Superintendent for Business
prufo@syossetschools.org
(516) 364-5651

December 16, 2019

New York State Education Department
Office of Audit Services, Room 524 EB
89 Washington Avenue
Albany, NY 12234

Dear Madam/Sir:

The comments contained in this letter collectively represent the corrective action plan for the Syosset Central School District in response to the two internal audit reports prepared by R.S. Abrams & Co. LLP for the 2018-19 school year.

Risk Assessment Update Report—We are pleased to report that of the 51 areas evaluated in the Risk Assessment, 48 were evaluated as low control risk and none were found to be high risk. Additionally, the two areas identified as moderate control risk last year: (1) Capital Assets - Inventory Tracking and (2) Food Services – Fund Balance improved to low risk in this year's report.

The findings, recommendations and corrective action from the 2018-19 risk assessment report are highlighted below.

IT - Disaster Recovery

- The auditors noted the district has not adopted a formal Disaster Recovery Plan. The District anticipates implementation of a plan by the start of the 2020-21 school year. Additionally, Syosset has two cybersecurity policies (AIG and NYSIR) that cover disaster recovery. Each policy has a specific disaster recovery plan tailored to the district. Each policy details the disaster recovery steps to take in the case of a breach, cyber, or ransomware attack. The District contracts with Nassau BOCES to manage our network infrastructure and BOCES provides a disaster recovery plan for this service. The district has contracted with Garnet River to implement a gap analysis of the network infrastructure to provide a road map to develop a comprehensive disaster recovery plan that will incorporate Education Law 2d, a template for access controls, and a process for NIST compliance.
- The report noted that the district has not verified the integrity of the accounting information system (AIS) backup performed by the vendor. Harris School Solutions performs nightly snapshot backups and Commvault agent-based backups of the district accounting information system: WinCap. WinCap data backups are executed in Indianapolis. The servers are located in Pittsburgh. Multiple locations for data warehousing is an industry standard for data redundancy and protection. Syosset performs Unitrends nightly backups of the AIS, Finance Manager, on the virtualized server VM-ZEUS. The Network Administrator and the K-12 Coordinator of Instructional and Administrative Technology receive daily backup status reports of all servers.

IT- Permissions/Access Controls

- The auditors noted that the district does not require passwords to be changed periodically and does not have a lockout policy in place. The District is currently implementing a self-service password reset system to allow users to reset their passwords remotely. This service will facilitate the periodic changing

of passwords as well as the ability to create longer, stronger passwords or passphrases of 20 characters or more. The District will be training staff members on the self-service password reset procedure and the stronger password procedure. The NIST Standards adopted by Education Law 2D does not recommend periodic, forced changing of passwords as this leads to users choosing weaker and easier passwords. Instead, the standard supports passphrases of at least 20 characters, special characters and, uppercase letters as a requirement. Aligned with the new secure password policy for the District, a lockout procedure will be implemented for the AIS and network.

- The auditors noted that 4 individuals have the ability to initiate and issue purchase orders. All four of the individuals are appointed by the BOE to serve as Purchasing Agents or Assistant Purchasing Agents. There were no instances of an individual both initiating a requisition and issuing a purchase order. To enhance internal controls, permissions have been modified so individuals that are appointed to issue purchase orders do not have rights to initiate a purchase requisition.

- The auditors noted eight user accounts in WinCap for which the date of last password change exceeded the 90 day threshold established by the District's AIS password policy. The eight user accounts in WinCap are accessed on an infrequent basis. For example, the Summer School Principal logs in once in July. For these 8 users, the next time the account accessed, a prompt will force them to reset their password. While the 90 day threshold is established and working for all accounts in WinCap we are reviewing the necessity of access for infrequent users.

- The auditors reported that one out of ten user accounts was not assigned to a specific individual and three out of ten accounts are associated with individuals who are no longer employed in the District. The IT department has taken corrective action by comparing active employees in WinCap to active network user accounts and deactivating accounts for past employees. Additionally, the district maintains a minimum amount of email accounts that are generic for public communications, and these accounts do not have network access. The district also has generic test accounts that have limited access to the network and are used to implement new security and organizational procedures.

Report on Internal Controls Related to Medical and Dental Benefits and Retiree Health Insurance—

- The in-depth report for 2018-19 focused on employee benefits. The auditors had no findings in the areas of Policies and Procedures, Health Declinations, Retirees Health Insurance, Dental Insurance and Flexible Spending Accounts. In the area of Health Insurance Coverage they noted 2 people that did not have documentation for dependent coverage and one of the two people did not have a completed enrollment form on file. The Benefits office is securing copies of the documentation as these employees were part of the insurer's dependent eligibility verification project that began in 2009. Currently, the benefits department uses a benefits check list for all new employees to ensure that the appropriate supporting documentation is available.

- The audit report indicated one occurrence of a retiree being over-paid a Medicare Part B reimbursement. The benefits department investigation found that the overpayment was the result of an unusual SS-1099 statement. As a result of this finding the benefits department checked all SS-1099s to ensure no other occurrences of this issue. Additionally, the Medicare Part B letter that the benefits office annually sends to all retirees has been amended to include a statement asking for additional documentation for spouses/domestic partners that are retirees of the railroad.

Sincerely,

Patricia Rufo