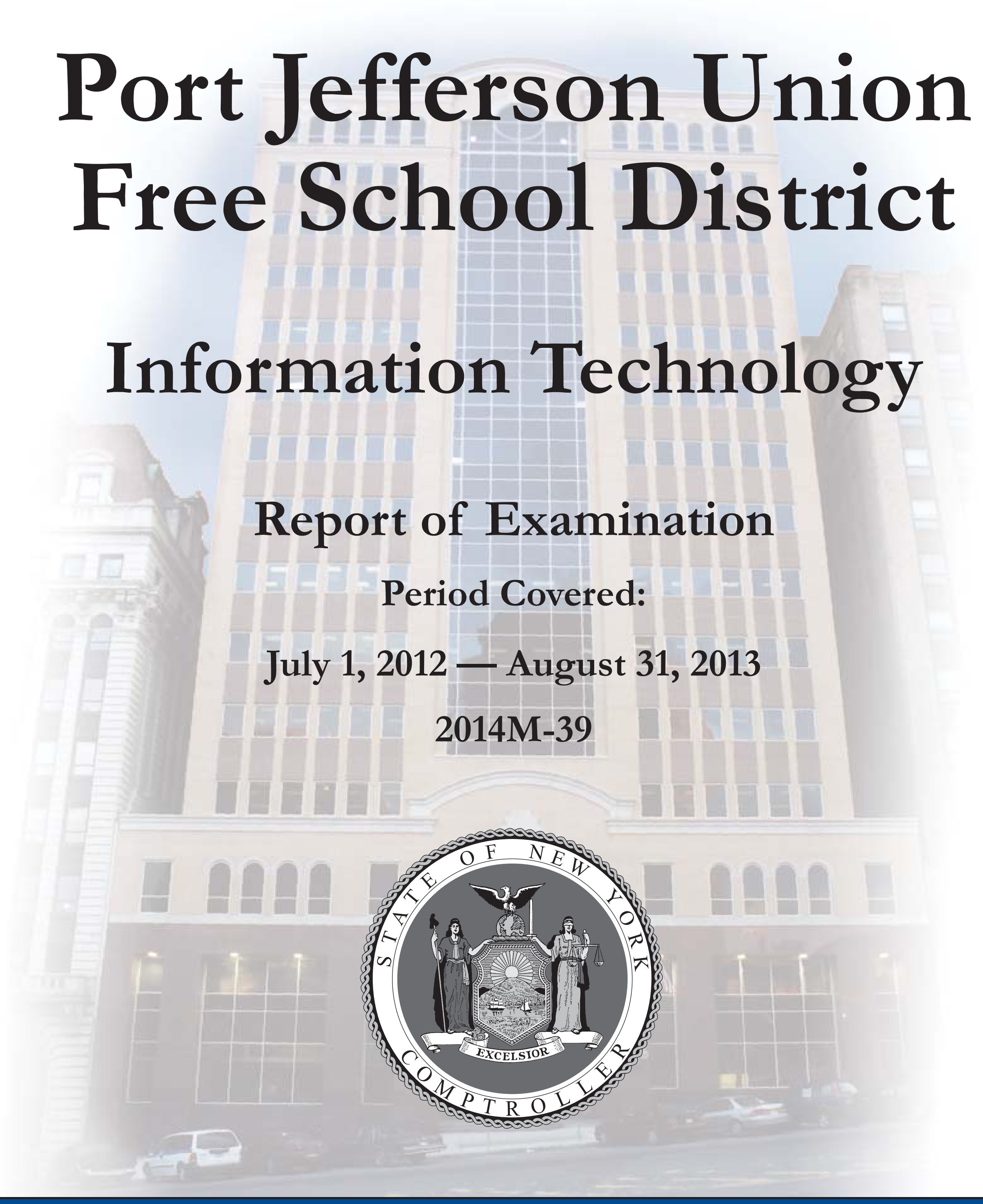
Office of the New York State Comptroller

Division of Local Government
& School Accountability



Port Jefferson Union Free School District

Information Technology

Report of Examination

Period Covered:

July 1, 2012 — August 31, 2013

2014M-39

Thomas P. DiNapoli

Table of Contents

Page

AUTHORITY LETTER 2

INTRODUCTION 3

Background 3
Objective 3
Scope and Methodology 3
Comments of District Officials and Corrective Action 4

INFORMATION TECHNOLOGY 5

Acceptable Use Policy 5
User Access Rights 6
Vendor Master File 8
Remote Access 9
Network Audit Trails 10
Physical Access 10
Inventory 11
Recommendations 12

APPENDIX A Response From District Officials 14
APPENDIX B Audit Methodology and Standards 16
APPENDIX C How to Obtain Additional Copies of the Report 18
APPENDIX D Local Regional Office Listing 19

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

April 2014

Dear School District Officials:

A top priority of the Office of the State Comptroller is to help school district officials manage government resources efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support district operations. The Comptroller oversees the fiscal affairs of districts statewide, as well as compliance with relevant statutes and observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations and the Board of Education governance. Audits also can identify strategies to reduce costs and to strengthen controls intended to safeguard district assets.

Following is a report of our audit of the Port Jefferson Union Free School District, entitled Information Technology. This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the General Municipal Law.

This audit's results and recommendations are resources for district officials to use in effectively managing operations and in meeting the expectations of their constituents. If you have questions about this report, please feel free to contact the local regional office for your county, as listed at the end of this report.

Respectfully submitted,

Office of the State Comptroller
Division of Local Government
and School Accountability

Introduction

Background

The Port Jefferson Union Free School District (District) is located in the Village of Port Jefferson in Suffolk County. It is governed by a Board of Education (Board) which comprises seven elected members. The Board is responsible for the general management of the District's financial affairs. The Superintendent of Schools (Superintendent) is the chief executive officer and is responsible, along with other administrative staff, for day-to-day management under the Board's direction.

The District operates three school buildings with approximately 1,200 students and 374 employees. Actual expenditures for the 2012-13 fiscal year totaled $36 million, which were funded primarily with real property taxes, State aid and PILOT payments.

District employees use networked computers in day-to-day operations for instructional purposes and to process financial transactions. The District has a Network and Systems Administrator who reports directly to the Assistant Superintendent for Business and is responsible for overseeing office automation equipment needs and selecting equipment and software to meet those needs. The District Treasurer (Treasurer) is responsible for all District moneys and has been charged with additional duties as both benefits administrator and system administrator of the District's financial software application.

Objective

The objective of our audit was to evaluate the District's information technology (IT) infrastructure. Our audit addressed the following related question:

- Did the Board and District officials adequately safeguard IT assets?

Scope and Methodology

We evaluated the District's IT oversight for the period July 1, 2012 through August 31, 2013. Our audit disclosed areas where additional IT security controls should be instituted. Because of the sensitive nature of some of this information, certain specific vulnerabilities are not discussed in this report, but have been separately communicated to District officials so they could take corrective action.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit is included in Appendix B of this report.

Comments of District Officials and Corrective Action

The results of our audit and recommendations have been discussed with District officials and their comments, which appear in Appendix A, have been considered in preparing this report.

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of the General Municipal Law, Section 2116-a (3)(c) of the Education Law, and Section 170.12 of the Regulations of the Commissioner of Education, a written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and forwarded to our office within 90 days. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. The Board should make the CAP available for public review in the District Clerk's office.

Information Technology

District officials are responsible for designing internal controls over information technology (IT) resources that include policies and procedures designed to protect software and data from loss or misuse due to errors, malicious intent or accidents. Such policies and procedures should include an acceptable computer use policy and should address using and monitoring the District's IT system by enabling and periodically reviewing audit trails. District officials should develop written procedures for adding, deleting and changing user access rights within the District's financial software and ensure that users have only those rights needed to complete their job duties. Further, the District should establish procedures to monitor and control remote access to the District's network by outside vendors and consultants. District officials also should ensure changes to the vendor master file are properly authorized and that vendors no longer used by the District are deactivated. Lastly, District officials must ensure that the District's computer assets are physically secured and tracked by maintaining a comprehensive, accurate inventory record that is periodically reviewed and updated.

The Board and District officials need to improve controls over the District's IT assets. The Board has not established a computer use policy for employees to define appropriate user behavior or procedures to ensure the security of the District's IT system. The Treasurer has administrative rights to the District's financial software that allow her to control and use all aspects of the financial software application, which creates the opportunity for the manipulation and concealment of transactions. Also, the District's vendor master file is outdated with inactive vendors and duplicate names for the same vendors.

In addition, the District has no controls in place over remote access, such as user authorizations, policies or monitoring, and has not enabled the audit trail function for its network operating system. Therefore, the District cannot ensure accountability for unauthorized users, reconstruction of events, intrusion detection, and problem identification. Finally, physical security over the District's server room is inadequate, and the District's computer asset inventory record is incomplete and inaccurate. As a result, the District's IT resources are subject to an increased risk of unauthorized access, manipulation, theft and loss.

Acceptable Use Policy

An acceptable use policy defines appropriate user behavior and the tools and procedures necessary to protect information systems. Such policies should include, among other things, procedures governing the acceptable use of computers, internet access, email and portable devices and procedures designed to protect the District's resources and confidential information. District officials should distribute acceptable computer use policies to all employees. It is important that such policies include provisions for enforcement and that system users acknowledge that they are aware of and will abide by the policy.

The Board has not adopted and implemented a comprehensive acceptable use policy or procedures to ensure the security of the District's IT system. Without a comprehensive policy that explicitly conveys the appropriate use of the District's electronic equipment, District officials cannot be assured that users are aware of their responsibilities, and officials do not have consistent standards by which to hold users accountable.

Although we did not find any inappropriate use of District computers, the District's lack of a computer use policy increases the risk that inappropriate computer use could occur – either intentionally or accidentally – and potentially expose the District to virus attacks or compromise systems and data, including key financial and confidential information.

User Access Rights

District officials should ensure that there are written procedures in place for granting, changing and terminating access rights to the overall networked computer system and to the specific software applications. These procedures should establish who has the authority to grant or change access (e.g., supervisory approval). Administrator rights allow users to create, delete and modify files, folders or settings, including assigning users' access rights. Generally, a system administrator is designated as the person who has oversight and control of the system and has the ability to add new users and change users' passwords and access rights. With this ability, administrators are able to control and use all aspects of the software. The administrator for the District's finance application should be an individual with no ties to the business office.

Also, to ensure proper segregation of duties and internal controls, it is important for the computer system to limit individual user access rights only to the functions necessary to fulfill their job responsibilities. Such access controls prevent users from being involved in multiple aspects of financial transactions and restricts unauthorized access that can lead to the intentional or unintentional change or destruction of financial data. When it is impractical to segregate incompatible duties, District officials must provide oversight of the work being performed to mitigate the risk created by the incompatible duties.

There are no written procedures to add, delete or modify an individual's access rights to the District's overall computer system. Access to the network is granted by the District's Network and Systems Administrator based solely on a verbal request or email from the human resources office. In 2006, the Board adopted a policy which requires a form be completed to add, delete or modify an individual's access rights to the financial software application. However, the District has not used this form since May 2008. Instead, during our audit period, access or access changes to the financial software application were granted based on an email from the Assistant Superintendent for Business.

There were 35 active user identifications (IDs) that had access to the financial software application during our audit period. Of the 35 users, we found that two no longer needed access to the software. Specifically, there is a user ID for an intern who no longer has a position at the District, and one employee had a second user ID which was no longer needed.

We also found that District officials did not designate an administrator who is independent of the financial recordkeeping functions. The Treasurer has administrative rights to the District's financial software that allow her to add new users and change users' passwords and access rights. With this ability, the Treasurer is able to control and use all aspects of the financial software application, which creates the opportunity for the manipulation and concealment of transactions.

Also, even if the Treasurer did not have administrative rights to the District's financial software, she would still need to have access to all of the modules of the financial software package based on her assigned job duties. The Treasurer's job duties include supervising the payroll clerk and reviewing the biweekly payroll. To carry out these duties, she needs the ability to add, delete and maintain employee attendance and make corrections to all payroll information, if necessary, after the payroll has been processed. These permissions are not compatible with her other assigned duties of disbursing funds and preparing bank reconciliations. Consequently, if District officials were to assign someone outside of the business office as the administrator of the financial software application, they still would need to provide oversight of work performed by the Treasurer to mitigate the risk created by her incompatible duties.

We also found that the accounts payable clerk is able to convert purchase requisitions to purchase orders, which is the purchasing agent's responsibility. These access rights are not compatible with the job duties of processing claims and purchase orders for payment and mailing checks after payments have been audited and approved. As a result, the District has an increased risk that purchase order and claim data can be intentionally changed or deleted.

Due to the improper assignment of administrative privileges and the lack of oversight of work performed by the Treasurer, the District has an increased risk that unauthorized changes to the accounting records, software security settings, and user authorization privileges could occur and remain undetected.

Vendor Master File

Within a computerized accounting system, the vendor master file contains a list of vendors from which District employees are permitted to purchase goods and services. Any changes to the vendor master file should be properly authorized. In addition, it is important that District management deactivate vendors that are no longer used. Also, District management should establish procedures to limit user access to the vendor master file to only the individual who is responsible for making changes to the vendor master list and should ensure that all former employees' access rights to the vendor master list are promptly removed.

The District's vendor master file contains 1,972 active vendors of which 1,360 received payments during our audit period. The District has not established procedures for adding, changing or deleting a vendor from the vendor master file. District management does not require any verification to determine if a vendor being added to the vendor list is already included in the vendor master file. Any one of three employees in the business office is able to add vendors and change vendor information. District officials told us that the procedure they follow to periodically review and purge inactive vendors is to review the file at the end of each school year and deactivate any vendor not used within the previous three-year period. However, we found that this procedure was not always followed.

We randomly[1] selected 30 vendors from the master vendor list and found that 17 were used during our audit period. Seven of the remaining 13 vendors were last used in the 2011-12 fiscal year. For the remaining six vendors, we found that two have never been used, three were last used in 2010 and one was last used in 2009.

We also found that the District had 63 vendor ID numbers for 28 vendors within the master file. District officials told us they required 17 of these vendors to have duplicate IDs for various reasons, such as to identify different divisions or departments within the same company. However, District officials were unable to provide any reason for the remaining 11 vendors to have duplicate ID numbers. The District paid $24,015 to these 11 vendors under these duplicate vendor ID numbers, rather than under the originally created vendor ID number, during our audit period.

[1] See Appendix B for methodology of sample selection.

Allowing inactive vendors to remain in the vendor master file increases the District's risk for improper payments and/or errors to occur and remain undetected. Further, because the District does not have any procedures in place to confirm whether a vendor is already in the system, this results in inaccurate vendor records and could lead to duplicate and/or inaccurate payments.

Remote Access

Remote access is the ability to access a network from the internet or other external source. It must be controlled and monitored so that only authorized individuals can use the District's computer system or retrieve data. District officials should establish policies and procedures that address how remote access is granted, who is given remote access and how remote access will be monitored and controlled. If remote access users are not District employees, but are instead IT consultants, District officials should establish service level agreements (SLA) with these consultants regarding expectations and consequences for violating such expectations. An SLA should clearly stipulate the contract period, the services to be provided, measurable targets of performance and the basis for compensation.

The Board has not established policies and procedures for remote access to ensure that computerized data is properly safeguarded. District officials granted remote access to the District's computer system to two vendors and nine District employees. The vendors and employees can access the District's computers at any time, without restriction. There are currently no controls in place, such as user authorizations, policies or monitoring, and the District does not have an SLA with either vendor.

One of the two vendors, an IT consultant, performs IT-related duties for the District, including upgrading all of the District's computer hardware, networks and operating systems. The vendor can access the District's computers at any time without restriction. The Assistant Superintendent for Business told us that the District did not enter into an SLA with this vendor because it obtained the vendor through a Board of Cooperative Educational Services cooperative services agreement. The other vendor, a computer software vendor, has access to one of the District's software applications. District officials told us that this vendor must first obtain authorization prior to remotely logging into the District's system. Although requiring this vendor to obtain authorization prior to logging in is a good control, the District still should have an SLA with this vendor to identify the vendor's contract period, services to be provided, measurable targets of performance and basis for compensation.

The Board's failure to develop policies and procedures for remote access with employees and vendors increases the District's risk that data could be lost, damaged or misused. Also, the Board's failure to enter into an SLA with its vendors contributes to a lack of accountability for who has responsibility for the various aspects of the District's IT environment and leaves routine contractual items undefined, including contract periods, expected provided services, performance targets and basis for compensation.

Network Audit Trails

The District's computer system should provide a means of determining, on a constant basis, who is accessing the system and what activity is occurring. Audit trails maintain a record of activity by system or application and by user. Audit trails help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection and problem identification. Maintaining and regularly reviewing audit trails enables District officials to determine who is accessing the network and whether the access is appropriate. Also, reviewing audit trails provides the District with the ability to trace questionable activity. District officials should implement procedures to periodically produce and review these audit trails.

Because of the unrestricted remote access, we requested audit trails from the District's network operating system for three specific dates[2] during our audit period. However, District officials told us the audit trail option had not been activated on its network operating system. The Network and Systems Administrator stated that by default this option is not enabled, and District officials had not chosen to enable it at that time. As a result, District officials are not monitoring whether any authorized users have initiated any inappropriate access to the District's network and/or whether any unauthorized users have accessed the network.

The failure of District officials to generate network operating system audit trails and to periodically examine the audit trail is a significant weakness that could allow unauthorized activities to occur and remain undetected.

Physical Access

Physical security over computerized assets is an important component of overall computer and data security. Limiting physical access to the server room to only authorized personnel is necessary to secure the District's computerized assets and data. Network components must be physically secured in a locked room with adequate ventilation where access is controlled and tracked. Security is enhanced by keeping server room doors locked at all times, controlling the keys, and documenting visitors' arrivals and departures.

[2] Refer to Appendix B for further information on our sample selection.

District officials have not adequately secured all of the District's IT hardware. Although the server room is located within a closet that can be locked by key, we found the server room door was not always locked. Further, District officials do not track physical access to the server room. On two occasions, we found the server room door unlocked with no other individual present in the building. After we brought this to the District's attention, the server room door was locked each subsequent time that we observed it. However, the District's Network and Systems Administrator told us that anyone who had a District master key could access the server room. District officials were unable to tell us how many individuals have a master key.

Under the existing conditions, it is difficult for the District to prevent unauthorized and/or malicious access to these assets or to identify the party responsible if such access did occur. Physical threats, whether internal, external, malicious or inadvertent, could lead to damaged or stolen hardware and/or information and the release of personal or confidential information. These security breaches can result in monetary loss and excessive staff hours to correct the problem.

Inventory

Good financial practices require that management maintain proper records of their equipment and perform a periodic physical inventory. Accurate and complete inventory lists help to ensure that inventories are accounted for properly. A detailed inventory record should include a description of each item, including make, model and serial number; the name of the employee to whom the equipment is assigned, if applicable; the physical location of the asset and relevant purchase information including acquisition date. Each item also should be affixed with identification tags for easy identification. The items should be periodically examined to establish their condition and to ensure they have not been misplaced or stolen. Equipment cannot properly be tracked and protected by District officials if officials do not know what equipment the District has and where the equipment resides.

We found the District's IT inventory record to be incomplete and inaccurate. The District's technology department maintains an inventory list of the computer equipment for each building. We attempted to verify the accuracy of this record by tracing computer items from the record to the physical assets. We initially chose to review nine items, seven desktop computers and two printers,[3] from the inventory list that were identified as being located in the operations and maintenance (O&M) building. We were able to physically observe five of the desktop computers, but were unable to locate the two printers and remaining two desktop computers. Also, while

[3] Refer to Appendix B for more information on our sample selection.

observing the computer equipment inventory in the O&M building, we identified an additional five IT assets that were not listed on the inventory record at all.[4]

Although the Network and Systems Administrator and Assistant Superintendent for Business told us that the District issues tablets to some of its employees, the inventory list did not include any tablets. District officials provided us with a list of 28 names of District employees who had been issued a tablet and two locations where 44 other tablets were located. However, this list did not contain any additional identifying information for these tablets, such as serial numbers.

Also, the tablets did not have any identification tags. Therefore, District officials would be unable to positively identify them as the 72 tablets originally purchased by the District. District employees who were issued tablets were not required to sign a form acknowledging their responsibility for the safety and return of the tablets.

Without an accurate inventory of computer and technology equipment and software, District officials cannot be assured that these assets are adequately accounted for and protected from loss, theft, misuse and obsolescence. Further, in the event of a disaster, the District would be unable to provide the insurance company with an accurate list of assets, and District officials would be unaware of what they needed to replace.

Recommendations

1. The Board should adopt and implement a comprehensive computer policy for IT operations that includes guidelines for acceptable use of equipment and systems by District personnel. This policy should be distributed to all District personnel.

2. District officials should develop written procedures for granting, changing, and terminating user access rights to the overall networked computer system and to specific software applications.

3. The Board should designate someone independent of business office operations to be the financial software system administrator.

4. District officials should assign user access rights to employees based on their job duties. If an employee has incompatible duties, District officials should provide oversight and review of the work performed by that individual.

5. District officials should establish procedures for maintaining

[4] Two desktop computers, two printers and one digital whiteboard

the vendor master file that include confirming that each vendor is unique within the system, periodically reviewing the vendor master file and deactivating vendors that are no longer used, and ensuring that vendor information is consistent and appropriate.

6. The Board should develop policies and procedures to address how remote access should be granted, who should be given remote access, and how District officials should monitor and control remote access. The District also should obtain written agreements with its remote access users to establish the District's needs and expectations, the level of system access allowed, contract period, services to be provided, measurable targets of performance and basis for compensation, where necessary.

7. District officials should monitor remote access provided to the District's IT vendor and evaluate whether the vendor's current access rights are appropriate and serve an appropriate business purpose.

8. The Board should require and District officials should ensure that the audit trail function is enabled within the District's network operating system. Also, District officials should establish procedures for periodically reviewing audit trails.

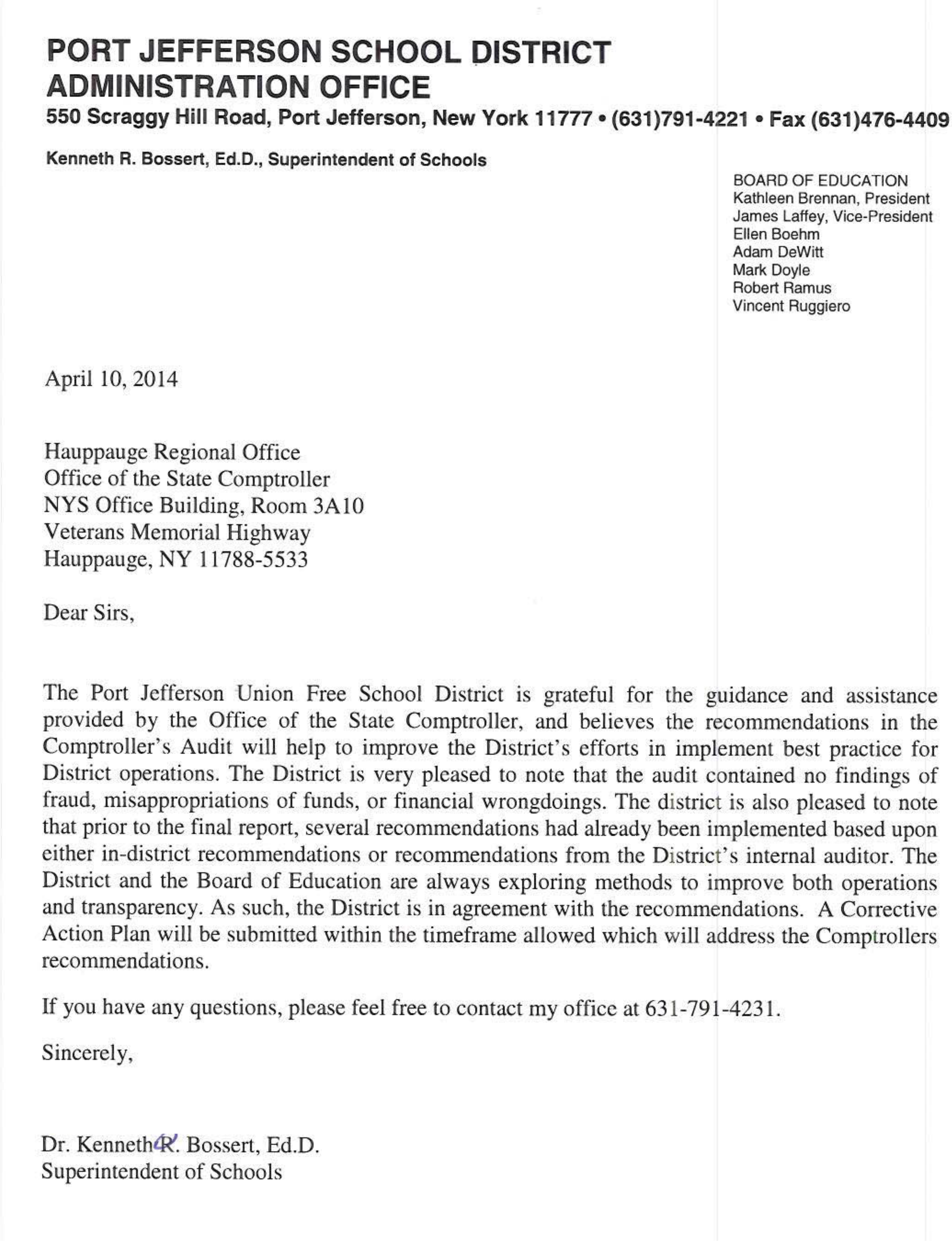
9. District officials should ensure the server room remains locked at all times, restrict physical access to the server room to only authorized individuals and record the arrival and departure dates and times of employees and visitors to-and-from the server room.

10. The Board should establish a comprehensive inventory policy that defines procedures for tagging all new purchases as they occur, relocating assets, updating the inventory list, performing periodic physical inventories and investigating any differences, and holding individuals accountable for safeguarding District assets that have been entrusted to them.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

The District officials' response to this audit can be found on the following page.



PORT JEFFERSON SCHOOL DISTRICT
ADMINISTRATION OFFICE
550 Scraggy Hill Road, Port Jefferson, New York 11777 • (631)791-4221 • Fax (631)476-4409

Kenneth R. Bossert, Ed.D., Superintendent of Schools

BOARD OF EDUCATION
Kathleen Brennan, President
James Laffey, Vice-President
Ellen Boehm
Adam DeWitt
Mark Doyle
Robert Ramus
Vincent Ruggiero

April 10, 2014

Hauppauge Regional Office
Office of the State Comptroller
NYS Office Building, Room 3A10
Veterans Memorial Highway
Hauppauge, NY 11788-5533

Dear Sirs,

The Port Jefferson Union Free School District is grateful for the guidance and assistance provided by the Office of the State Comptroller, and believes the recommendations in the Comptroller's Audit will help to improve the District's efforts in implement best practice for District operations. The District is very pleased to note that the audit contained no findings of fraud, misappropriations of funds, or financial wrongdoings. The district is also pleased to note that prior to the final report, several recommendations had already been implemented based upon either in-district recommendations or recommendations from the District's internal auditor. The District and the Board of Education are always exploring methods to improve both operations and transparency. As such, the District is in agreement with the recommendations. A Corrective Action Plan will be submitted within the timeframe allowed which will address the Comptrollers recommendations.

If you have any questions, please feel free to contact my office at 631-791-4231.

Sincerely,

Dr. Kenneth R. Bossert, Ed.D.
Superintendent of Schools

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

Our overall goal was to assess the adequacy of the internal controls put in place by officials to safeguard District assets. To accomplish this, we performed an initial assessment of internal controls so that we could design our audit to focus on those areas most at risk. Our initial assessment included evaluations of the following areas: financial oversight, cash receipts and disbursements, purchasing, asset management, payroll and personal services, and information technology (IT).

During the initial assessment, we interviewed appropriate District officials, performed limited tests of transactions, and reviewed pertinent documents, such as Board minutes and financial records and reports. Further, we reviewed the District's internal controls and procedures over the computerized financial databases to help ensure that the information produced by such systems was reliable.

After reviewing the information gathered during our initial assessment, we determined where weaknesses existed and evaluated those weaknesses for risk of potential fraud, theft and/or professional misconduct. We then decided on the reported objective and scope by selecting for audit those areas most at risk. We selected IT for further audit testing.

To accomplish our audit objective and to obtain valid audit evidence, our audit procedures included the following:

- We reviewed the District's IT policies and procedures.

- We interviewed the Network and Systems Administrator, Treasurer/Benefits Administrator and Assistant Superintendent for Business regarding the IT system and financial software. These discussions included inquiries regarding policies and procedures, user access rights, audit logs, user permissions, vendor accounts, remote access and inventories.

- We reviewed the master vendor list for duplicate vendors.

- We used the random number generating formula to choose a sample of 30 vendors. The formula gave us the number of the vendor that we started with. From that point on, based on a population of 1,972 vendors, we chose every 66th vendor. We then compared the selected vendor master file names to the District's computer data to determine whether vendors were active or inactive based on whether the District used them during our audit period and/or the year prior to our audit period. We did an internet search for the name of the vendor's personal and company name for more information and followed up with the Assistant Superintendent for Business on any items that appeared inconsistent with the District's data.

- For six of 30 vendors that were on the District's master vendor list but had not been used by the District during our audit period, we requested information on each vendor to determine when they were last used, what type of purchase was made and why they were still active vendors. We also reviewed information in the District's master vendor list related to 28 vendors that had duplicate names and/or addresses representing 63 vendor ID numbers.

- We reviewed a list of all 44 users of the financial software, consisting of 35 active and nine disabled accounts, and the account access rights for all 44 users to determine if their access to the financial software was consistent with their job responsibilities. We also reviewed the list to determine if default accounts had been removed and to ensure that only active employees had access to the software.

- We obtained audit logs for the financial software and reviewed them to ensure that users were performing only those duties that were related to their job responsibilities and permissions. We judgmentally selected to review the audit logs generated for September 28, 2012 (the first payroll of the school year), June 17, 2013 (the Monday of the last day of school), July 20, 2013 (the day after the District was notified that we were doing an audit, and it was on a weekend), and July 22, 2013 (the first business day after the District was notified of our upcoming audit). We were unable to view the audit logs for the District's network operating system because the audit trail option had not been activated on its network system.

- We observed the server room for physical security on several occasions.

- We judgmentally selected nine inventory items based on the location where we were physically working within the District.

We conducted this performance audit in accordance with GAGAS. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX C

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller
Public Information Office
110 State Street, 15th Floor
Albany, New York 12236
(518) 474-4015
http://www.osc.state.ny.us/localgov/

APPENDIX D

OFFICE OF THE STATE COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY

Andrew A. SanFilippo, Executive Deputy Comptroller
Gabriel F. Deyo, Deputy Comptroller
Nathaalie N. Carey, Assistant Comptroller

LOCAL REGIONAL OFFICE LISTING

BINGHAMTON REGIONAL OFFICE
H. Todd Eames, Chief Examiner
Office of the State Comptroller
State Office Building - Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313
Email: Muni-Binghamton@osc.state.ny.us

Serving: Broome, Chenango, Cortland, Delaware,
Otsego, Schoharie, Sullivan, Tioga, Tompkins Counties

BUFFALO REGIONAL OFFICE
Robert Meller, Chief Examiner
Office of the State Comptroller
295 Main Street, Suite 1032
Buffalo, New York 14203-2510
(716) 847-3647 Fax (716) 847-3643
Email: Muni-Buffalo@osc.state.ny.us

Serving: Allegany, Cattaraugus, Chautauqua, Erie,
Genesee, Niagara, Orleans, Wyoming Counties

GLENS FALLS REGIONAL OFFICE
Jeffrey P. Leonard, Chief Examiner
Office of the State Comptroller
One Broad Street Plaza
Glens Falls, New York 12801-4396
(518) 793-0057 Fax (518) 793-5797
Email: Muni-GlensFalls@osc.state.ny.us

Serving: Albany, Clinton, Essex, Franklin,
Fulton, Hamilton, Montgomery, Rensselaer,
Saratoga, Schenectady, Warren, Washington Counties

HAUPPAUGE REGIONAL OFFICE
Ira McCracken, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788-5533
(631) 952-6534 Fax (631) 952-6530
Email: Muni-Hauppauge@osc.state.ny.us

Serving: Nassau and Suffolk Counties

NEWBURGH REGIONAL OFFICE
Tenneh Blamah, Chief Examiner
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725
(845) 567-0858 Fax (845) 567-0080
Email: Muni-Newburgh@osc.state.ny.us

Serving: Columbia, Dutchess, Greene, Orange,
Putnam, Rockland, Ulster, Westchester Counties

ROCHESTER REGIONAL OFFICE
Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street – Suite 522
Rochester, New York 14614-1608
(585) 454-2460 Fax (585) 454-3545
Email: Muni-Rochester@osc.state.ny.us

Serving: Cayuga, Chemung, Livingston, Monroe,
Ontario, Schuyler, Seneca, Steuben, Wayne, Yates Counties

SYRACUSE REGIONAL OFFICE
Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428
(315) 428-4192 Fax (315) 426-2119
Email: Muni-Syracuse@osc.state.ny.us

Serving: Herkimer, Jefferson, Lewis, Madison,
Oneida, Onondaga, Oswego, St. Lawrence Counties

STATEWIDE AUDITS
Ann C. Singer, Chief Examiner
State Office Building - Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313