Office of the New York State Comptroller

Division of Local Government
& School Accountability

Greenville Central School District

Information Technology

Report of Examination

Period Covered:

July 1, 2014 – January 14, 2016

2016M-221

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

September 2016

Dear School District Officials:

A top priority of the Office of the State Comptroller is to help District officials manage school district 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 school 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 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 Greenville Central 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 New York State 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 Greenville Central School District (District) is located in the Town of Greenville in Greene County. The District is governed by the Board of Education (Board), composed of seven elected members. The Board is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools is the District's chief executive officer and is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction.

The District operates an elementary and a middle-high school, with an enrollment of approximately 1,200 students. The District's budgeted appropriations for the 2014-15 and 2015-16 school years were $28.6 million and $28.7 million, respectively.

The District contracts with the Questar III Board of Cooperative Educational Services (BOCES) for educational and information technology (IT) services and resources. IT services are provided by the Northeastern Regional Information Center (NERIC). These services include Internet access, web content filtering, data warehousing and financial/human resource management software. In addition, the District employs three IT staff members: a Director of Technology, a Network Administrator and a Technology Assistant for day-to-day IT operations.

Objective

The objective of our audit was to evaluate the District's internal controls over IT. Our audit addressed the following related question:

- Are internal controls over IT appropriately designed and operating effectively?

Scope and Methodology

We examined the District's IT internal controls for the period July 1, 2014 through January 14, 2016. We extended our review of data extracted from the District's computers and networks through April 8, 2016, the end of our fieldwork. Because of the sensitivity of some of this information, we did not discuss all the results in this report, but instead communicated them confidentially to the Board and District officials.

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 are included in Appendix B of this report. Unless otherwise indicated in this report, samples for testing were selected based on professional

judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

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. District officials generally agreed with our recommendations and indicated they have begun to initiate corrective action.

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of General Municipal Law, Section 2116-a (3)(c) of New York State 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 provided to our office within 90 days, with a copy forwarded to the Commissioner of Education. 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

The District uses IT to initiate, process, record and report transactions. It also relies on its IT systems for Internet access, email and maintaining financial and personal records. Therefore, the IT system and data are valuable resources. If the IT system is compromised, the results could range from inconvenient to catastrophic and require extensive effort to evaluate and repair. District officials are responsible for designing internal controls over the IT environment and resources. District officials should create policies and procedures designed to protect software, hardware and data from loss or misuse due to errors, malicious intent and accidents. Additionally, 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 have not ensured internal controls over IT are appropriately designed and operating effectively. The Board did not establish adequate IT policies and procedures. District officials did not maintain accurate and up-to-date IT hardware inventory records. We also found that service level agreements (SLA) for IT consultants do not adequately identify who is responsible for various aspects of the District's IT environment. District officials have also not ensured that District employees received adequate cyber security training. Finally, we identified significant weaknesses in the District's web filter and its implementation. As a result, the Board does not have adequate assurance that the District's IT assets are secure.

Policies and Procedures

Policies and procedures over IT are part of the internal control structure and provide criteria and guidance for the District's computer-related operations. Effective protection of computing resources and data includes the adoption of an acceptable use policy that informs users about appropriate and safe use of District computers, an online banking policy which protects District funds, a hardware sanitization policy which ensures that equipment is not discarded with sensitive data, a breach notification policy in the event that sensitive data is compromised and a disaster recovery plan with guidance for minimizing loss and restoring operations should a disaster occur. The Board should periodically review and update these policies as necessary to reflect changes in technology or the District's computing environment. Computer users need to be aware of security risks and be properly trained in practices that reduce the internal and external threats to the network.

The Board has not established adequate policies to ensure internal controls over IT are appropriately designed and operating effectively. Specifically, the District does not have adequate policies and procedures in the following IT areas:

Acceptable Use – Although the District has established an acceptable use policy and procedures, they have not been updated since September 2001. Further, personal use of IT assets is not clearly defined. For example, the policy does not address student or faculty use of take-home computers or tablets while offsite. Because this is not addressed in the acceptable use policy, there is no requirement in place to ensure they are used in an appropriate and secure manner, which could potentially expose the District to malicious attacks or compromise systems and data.

Breach Notification Policy – An individual's private or financial information, along with confidential business information, could be severely impacted if security is breached or personal data is improperly disclosed. It is a good practice for school districts to adopt a breach notification policy to detail how district officials would notify individuals whose private information was, or is reasonably believed to have been, acquired by a person without a valid authorization. The disclosure should be made in the most expedient time possible, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and reasonably restore the data system's integrity. The Board has not adopted a breach notification policy. As a result, in the event that private information is compromised, district officials and employees may not be prepared to notify affected individuals.

Sanitization and Disposal of Equipment – The Board has not adopted policies or procedures for sanitizing hard drives or other electronic media before disposing of them or for securing equipment intended for disposal. If sensitive and confidential information is not fully removed, it may be recovered and inappropriately used or disclosed by unauthorized individuals with access to the discarded equipment and media. We observed large amounts of out-of-service IT equipment left unsecured in the hallway, waiting to be disposed of. This equipment may contain personal, private or sensitive information. As a result, District IT data and assets are at risk of loss.

Disaster Recovery Plan – The Board is responsible for developing and documenting a disaster recovery plan. A good disaster recovery plan addresses a range of potential disruptions. These may include relatively minor disruptions, such as temporary power failures, as well as major disasters, such as fire or natural disasters, that would require reestablishing operations at a remote location. If controls

are not adequate, even relatively minor disruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts and inaccurate or incomplete financial or management information. Further, the plan should set forth procedures to ensure District personnel can either maintain or quickly resume mission-critical functions.

Although the District has a disaster recovery plan, it is not kept up to date, not properly distributed and not tested on a regular basis. The District's Disaster Recovery Team is responsible for implementing and maintaining the plan but does not include a current listing of personnel. Also, District officials have not tested the plan in over two years and the plan is not adapted to meet changing conditions. Furthermore, the District does not have proper procedures in place to actively respond in the event the District's network is compromised.

Web Filter

Due to the global nature of the Internet, school districts today find that it is a nearly indispensable resource for conducting legitimate business and educational activities. However, in recent years, even experienced users have been susceptible to significant threats from cybercriminals who exploit the vulnerabilities of systems and software to gain unauthorized access to sensitive data.

For example, computers can be infected by malicious software[1] that, unknown to users, installs a keystroke logger that captures computer user identification and password information. Hackers can later use this information to access networks, databases and even bank accounts, resulting in high risk of loss. Internet browsing increases the likelihood that users will be exposed to some form of malicious software that may compromise data confidentiality. The District should ensure there is an adequate web filtering process in place to limit vulnerabilities in District IT assets through web browsing and to ensure the District's network is only used for appropriate educational purposes.

The District's web filter, which is a purchased service from NERIC, needs to be improved. The District's web filter classifies websites into categories (Figure 1). The District can choose to either block

[1] Malicious software (malware) is designed to infiltrate a computer system by circumventing network defenses, avoiding detection and resisting efforts to disable it. Malware includes computer viruses, Trojan horses, spyware, worms, rootkits and other forms of invasive contaminating software. It can be introduced to a computer system through, for example, web browsers and email attachments. It may also be disguised as genuine software coming from an official Internet site. After installation, malware can thwart intrusion detection systems. Malware can be used to steal confidential or personal information like social security numbers, credit card numbers, computer user identification and passwords and bank account information. Malware can target individual users, organizations and networks.

or allow each of these categories based on the user.[2] There is also a public network, which is viewable by anyone in range. We found that students are not allowed to view several categories such as R-rated material, chat and alcohol on the secure network. However, the District's public network allows a student or other network user to disconnect from the secure network, connect to the public network and bypass the web filter to view blocked categories.

The District's acceptable use policy provides employees and students with guidelines for IT asset use and security. Specifically, the policy prohibits the use of District computers for noneducational or illegal purposes. However, we found examples of viewable web filter categories that did not appear to be for educational purposes. For example, users can access Internet radio, fantasy sports, games, tickets, weapons and travel websites. Further, teachers can access shopping and online auction sites.

To evaluate web usage, we examined 10 District computers' web histories.[3] We searched for website categories that appeared to be personal in nature rather than educational. As depicted in Figure 1, District staff were able to access websites unrelated to District activities, such as online banking, a music festival, an automobile dealership, insurance, personal email and social media. Although the acceptable use policy does not permit noneducational use, the web filter does not block categories that are frequently used for personal purposes.

Figure 1: Select Web Filter Categories

Content Filter Category	Content Group Viewable by			
	Public Network	Student Users	Non-Teacher Faculty	Teachers
R-Rated	X			X
Internet Radio	X	X	X	X
Sports Streaming	X	X	X	X
Entertainment	X	X	X	X
Movies and Television	X	X	X	X
Games	X	X	X	X
Chat	X			
Fantasy Sports	X	X	X	X
Shopping	X			X
Alcohol	X			
Tobacco	X	X	X	X
Weapons	X	X	X	X
Tickets	X	X	X	X

[2] The users are grouped by students, non-teacher faculty and teachers.

[3] See Appendix B, Audit Methodology and Standards, for details on our sample selection.

When employees and students access websites through the District's network, productivity is reduced and there is an increased risk that the websites' contents could put District assets and users at risk.

IT Inventory

Good business practices require management to maintain proper records of IT assets and perform a periodic physical inventory. Accurate and complete inventory lists help to ensure that assets 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 and asset value. Each item also should also be affixed with identification tags. Equipment should be periodically examined to establish condition and to ensure nothing has been misplaced or stolen.

The District needs to improve controls over its IT asset inventory. We obtained copies of the District's IT inventory and selected a judgmental sample of 119 assets out of 1,985 total assets over four locations to test the inventory for accuracy and completeness. We found a laptop cart in a classroom with all of the laptops left out that was supposed to contain 25 laptops. One of the laptops was missing from the cart but later located after we brought it to officials' attention. We located the remaining 93 of 94 assets without exception.

We also identified three pieces of equipment that were tagged but not included on the District's inventory list for those four locations. These tag numbers were missing from the sequence. The IT Director stated that these omissions were errors.

The District had 31 sequence gaps, indicating that it was missing 31 of its 1,985 tags (2 percent) from its asset inventory. Eleven missing tags were linked to specific assets totaling approximately $3,500, which we were able to locate. Examples of these items include a printer, wireless access points, a laptop and a monitor. The remaining 20 asset tags or tagged items are missing from the District's inventory listing, and District officials do not know what the assets are or the status of the tags or items. It is possible that these items are missing or were stolen, or that the tags were destroyed but not accounted for, on the District's log of destroyed asset tags.

Without an accurate inventory of IT hardware, District officials cannot be assured that these assets are adequately accounted for and protected from loss, theft and misuse. Furthermore, in the event of a disaster, the District would not be able to provide an accurate inventory for insurance purposes. Poor internal controls over the custody of IT assets diminishes accountability and exposes the District to increased risk for IT assets.

Service Level Agreements

To protect the District and avoid potential misunderstandings, there should be a written agreement between the District and its IT service provider that identifies the District's needs and expectations and specifies the level of service to be provided. The components of the SLA should include identifying the parties to the contract, definitions of terminology, term/duration of the agreement, scope/subject limitations, service level objectives and performance indicators, roles and responsibilities, nonperformance impact, security procedures, audit procedures, reporting requirements, review/update process, approvals, pricing, billing and terms of payment. This contract should be reviewed by knowledgeable IT staff, legal counsel or both and periodically be reviewed, especially if the IT environment or needs change significantly. Furthermore, contracts should establish measureable performance targets so that there is a mutual understanding of the nature and required level of service to be provided.

The District does not have a written SLA with BOCES or NERIC, its Internet, web filtering and data warehousing providers. The District chooses its services in a piecemeal fashion, selecting services needed for operations. The services provided are not comprehensive. The District does not know what services are provided upon purchase (other than the excerpt describing the product on NERIC's website). As a result, in the event of any failure of District IT controls (such as an IT breach, failure in content filters, IT inventory discrepancy, etc.), the lack of a specific SLA can contribute to confusion over who has responsibility for various aspects of the IT environment (i.e., the District or contractor), which ultimately puts the District's data and computer resources at greater risk.

Cyber Security Training

District policy states that the Superintendent or his or her designee shall provide training for those employees supervising students so that students who use the network receive training in the proper use of the network. The IT security community often identifies people as the weakest link in the chain to secure data and systems. Good internal controls should include District-wide IT security training and awareness efforts that are closely tied to the District's IT policies. The District cannot protect the confidentiality, integrity and availability of its data and computer systems without ensuring that the people who use and manage IT understand organizational IT security policies and procedures and their roles and responsibilities related to IT security.

The Board has not created adequate policies and procedures to ensure District employees receive proper cybersecurity training to protect District IT assets. The District requires students and their legal guardians to sign off on an acceptable use policy. However, the District does not provide the faculty with a formal document to sign

and does not require the faculty to attend any formal cybersecurity awareness training.

Recommendations

The Board should:

1. Update the District's acceptable use policy to include the use of personal devices on the District's network and acceptable use of District assets when used outside the District's network.

2. Develop IT policies for breach notification and sanitization and disposal of equipment. The Board also should ensure that the disaster recovery policy is periodically updated.

3. Adjust the web content filtering to ensure that staff and students are in compliance with the District's acceptable use policy.

4. Establish a comprehensive inventory policy that defines procedures for tagging all new purchases as they occur, relocating assets, updating the inventory list and performing periodic physical inventories.

5. Establish written agreements with service providers that state the District's needs and expectations and specify the level of service to be provided.

6. Ensure all network users receive IT security training.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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

GREENVILLE
CENTRAL SCHOOL DISTRICT

Tammy J. Sutherland
Superintendent of Schools

Jacqueline O'Halloran
District Clerk

September 12, 2016

Office of the State Comptroller
Newburgh Regional Office
33 Airport Center Drive, Suite 103
New Windsor, New York 12553

Re: Response to preliminary draft findings of audit report titled Information Technology

To the Office of the State Comptroller:

This letter is to acknowledge the receipt of the draft report titled Information Technology 2016M-221-IT for the period of July 1st, 2014 to April 8th, 2016 issued by the NYS Office of the State Comptroller for the Greenville Central School.

The results of the audit were found to be both fair and informative and we embrace this opportunity to make the necessary improvements to our practices and to formalize some of our unwritten procedures. In fact, the District has already begun to address the recommendations given in your report. Four (4) of the six (6) recommendations are related to Board Policy. As explained during the audit, the District and Board of Education have been working on a complete policy review. It is estimated that the Board will approve policies including the ones mentioned in the audit within the next few months. The District will make sure these policies contain the suggestions that you have made and that they are followed.

The District will prepare and send the appropriate Corrective Action Plan for all items listed in the report detailing how the District will implement the recommendations listed in the audit.

On behalf of the Greenville Central School District and Board of Education, we would like to thank the Office of the State Comptroller field staff involved for both their comprehensive and meaningful report and for their professionalism throughout the audit process.

Sincerely,

Tammy J. Sutherland
Superintendent of Schools

TJS:jo

P.O. BOX 129 • GREENVILLE, NY 12083-0129 • 518.966.5070 • FAX: 518.966.8346 • www.greenville.k12.ny.us

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

To achieve our audit objective and obtain valid evidence, we performed the following procedures:

- We interviewed District officials to obtain an understanding of the District's IT operations.
- We reviewed District records for any IT-related policies and procedures.
- We obtained reports from the District's web filter to review categories available and the groups categories are available to.
- We obtained a list of staff for the entire District and judgmentally selected 10 computers to run IT-related tests. The sample selected was based on access rights to various software programs and corresponding job duties. We reviewed the installed software and Internet browsing history on each computer.
- We reviewed Internet browsing history for use outside of the District's policy.
- We obtained and reviewed software permission reports to determine adequacy. In addition, we used these permission reports to verify users in the Active Directory; all users with permissions should have a corresponding notation.
- We reviewed documentation relating to services being provided by service providers and interviewed officials to determine if contracts or agreements exist.
- We conducted testing of IT-related assets for inventory completeness and accuracy.

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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

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
Tracey Hitchen Boyd, 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
Jeffrey D. Mazula, 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