DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2022M-73

Liberty Central School District

Information Technology

SEPTEMBER 2022

OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights **1**

Information Technology **2**

Why Should the Board and Officials Manage User Accounts? 2

The Board and Officials Did Not Adequately Manage Network User Accounts 2

Why Should Officials Have an IT Contract and a Service Level Agreement (SLA)? 3

The District Did Not Have Adequate IT Contracts and SLAs 3

Why Should the Board Adopt an IT Contingency Plan? 4

The Board's Adopted IT Contingency Plan Was Not Up to Date . . . 4

Why Should Officials Provide IT Security Awareness Training? 5

Employees Were Not Provided Adequate IT Security Awareness Training 5

What Do We Recommend? 6

Appendix A – Response From District Officials **7**

Appendix B – Audit Methodology and Standards **9**

Appendix C – Resources and Services **10**

Report Highlights

Liberty Central School District

Audit Objective

Determine whether the Liberty Central School District (District) Board of Education (Board) and District officials adequately safeguarded computerized data from unauthorized use, access and loss.

Key Findings

The Board and District officials did not adequately safeguard computerized data from unauthorized use, access and loss. In addition to sensitive IT control weaknesses that were communicated confidentially to officials, officials did not:

- Disable unnecessary network user accounts. As a result, the District's risk of a system compromise is increased.
- Establish adequate information technology (IT) contracts with the District's vendors. As a result, the roles and responsibilities of each vendor providing services may not be understood and the District may pay for duplicated services.
- Ensure the IT contingency plan was kept up to date. As a result, in the event of a cyberattack or disaster, officials may not be able to restore critical IT systems, applications or data timely.
- Provide users with comprehensive IT security awareness training. As a result, employees may not be prepared to recognize and appropriately respond to suspicious system activity.

Key Recommendations

- Regularly review network user accounts and disable unnecessary accounts.
- Establish adequate IT contracts, update the IT contingency plan and provide IT security awareness training.

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

Background

The District is located in the Towns of Bethel, Fallsburg, Liberty, Neversink, Rockland and Thompson in Sullivan County.

The District is governed by a nine-member Board responsible for the general management and control of the District's financial and education affairs. The Superintendent of Schools (Superintendent) is the chief executive officer responsible for the District's administration.

The District contracts with two third-party vendors to provide IT services, including network administration and the overall management of the District's IT infrastructure.

Quick Facts	
Network User Accounts	3,159
Non-student Accounts	630
Contracted IT Service Cost in our Audit Period	$514,628

Audit Period

July 1, 2020 – January 31, 2022

Information Technology

Why Should the Board and Officials Manage User Accounts?

Network user accounts enable the system to recognize specific users, grant authorized access rights and provide accountability by affiliating user accounts with specific users. User accounts are potential entry points for attackers because they could be used to access data and view personal, private and sensitive information (PPSI).[1] To help minimize the risk of unauthorized access, school district officials should actively manage user accounts including their creation, use and dormancy, and regularly monitor them to ensure they are appropriate and authorized. When user accounts are no longer needed, they should be disabled in a timely manner. A school district should have written policies and procedures for granting, changing, and removing user access to the network.

In addition, generic accounts may be needed for certain network services or applications to run properly but should be limited in use as they are not linked to individual users and, therefore, may have reduced accountability. For example, generic accounts can be created and used to scan student test scores. School district officials should limit the use of generic accounts and routinely evaluate the need for them and disable those that are not related to a specific academic or system need.

School district officials should limit the use of generic accounts and routinely evaluate the need for them. ...

The Board and Officials Did Not Adequately Manage Network User Accounts

One of the IT vendor's staff manage and maintain the District's network access and add, remove and modify user access from the network. However, officials have not developed comprehensive procedures for regularly reviewing user accounts and disabling those that are unnecessary.

We reviewed all of the District's 630 nonstudent network user accounts and identified 79 nonstudent network user accounts (13 percent) that were unneeded and should have been disabled, including 44 generic accounts that were disabled based on our inquiry with IT staff, and 43 network user accounts for former employees or third-party users. We identified an additional 35 generic accounts that IT staff were unsure whether they were needed and planned to investigate further. Many of the unneeded accounts had not been used in more than six months. During our audit fieldwork officials indicated they had begun disabling certain accounts and investigating other accounts.

The Superintendent acknowledged weaknesses in the on and offboarding of staff user access. During our fieldwork there was an external auditor performing

[1] PPSI is any information where unauthorized access, disclosure, modification, destruction or use – or disruption of access or use – could have or cause a severe impact on critical functions, employees, customers, third parties or other individuals or entities.

a review of the District's human resources processes. Officials said that work would result in developing a more streamlined process for adding, deleting, and modifying user access.

Unneeded network user accounts can be potential entry points for attackers and could be used to inappropriately access and view student or employee PPSI. This increases the risk that the PPSI could be changed intentionally or unintentionally or used inappropriately.

Why Should Officials Have an IT Contract and a Service Level Agreement (SLA)?

A school district board should have a written contract or agreement with its IT provider that indicates the contract period, services to be provided and basis of compensation for those services. In addition, to protect the school district and avoid potential misunderstandings, officials should have a separate written SLA between the school district and its IT provider that identifies the school district's needs and expectations and specifies the level of service to be provided.

An SLA establishes comprehensive, measurable performance targets so that there is a mutual understanding of the nature and required level of services to be provided. It provides detailed explanations of the services to be performed by identifying the parties to the contract and defining terminology; term or duration of the agreement; scope and/or subject limitations; service level objectives; performance indicators; roles and responsibilities; nonperformance impact; security and audit procedures; reporting requirements; review, update and approval processes; and scope of services to be provided.

The District Did Not Have Adequate IT Contracts and SLAs

The District paid two IT service providers $514,628 during our audit scope period to provide managed IT services. These services are provided as part of cooperative services agreements with the Eastern Suffolk Board of Cooperative Educational Services (BOCES) and the Putnam Northern Westchester BOCES.

While the District has IT contracts with both providers, because the contract language does not clearly identify the roles and responsibilities the vendors are to be providing, gaps in IT security practices may occur. The Board and District officials have the responsibility to ensure that any contracts with IT vendors adequately address the safety and security of District data. This can be achieved through specific language in the contracts and by a deliberate process of determining, through discussion with the vendor, how security will be achieved.

We were provided both vendor agreements and found they lacked language detailing the performance related to data security and did not provide for comprehensive, measurable performance targets so that there is a mutual understanding of the nature and required level of services to be provided. Furthermore, we were unable to determine whether duties were being duplicated by the providers.

Without defined language, the roles and responsibilities of each vendor providing services to the District may not be adequately understood by District officials and the District may be paying for services that are duplicated by the vendors. For example, both agreements include responsibilities that may overlap (Figure 1).

Figure 1: IT Vendor Responsibilities

IT Vendor A	IT Vendor B
Create learning resources for staff	Educate District employees on compliance requirements
Assist Superintendent with Implementation of the District's Technology Plan-Infrastructure	Assist in the implementation of policies and procedures

Why Should the Board Adopt an IT Contingency Plan?

To minimize the risk of data loss or suffering a serious interruption of service, school district officials should establish a comprehensive written IT contingency plan. The plan should address the potential for sudden, unplanned disruptions (e.g., ransomware or other malware attack, inadvertent employee action or fire) that could compromise the network and the availability or integrity of the school district's IT system and data, including its applications and PPSI.

Typically, an IT contingency plan involves analyzing business processes and continuity needs, identifying roles of key individuals and necessary precautions to maintain or quickly resume operations. It should also reference how the school district should back up its computer systems. Backup data should be stored at a secure offsite location, maintained off-network, encrypted and routinely tested to ensure its integrity. The plan should also be periodically tested, shared and updated to ensure key officials understand their roles and responsibilities during an unplanned IT disruption and to address changes in security requirements.

The Board's Adopted IT Contingency Plan Was Not Up to Date

Although the District has an adopted written IT contingency plan, it was outdated and not regularly reviewed to ensure pertinent information was updated. The plan was created in February 2018 and included an appendix of key contacts that included multiple individuals who were no longer District or IT vendor employees. For example, of the 16 contacts listed in the appendix, eight contacts were no longer with the District. These contacts are an important part of the plan since, depending on the severity of network outage, individuals would be contacted in sequential order to start the process of restoring services as soon as possible. An outdated contact list only adds to the time the network could be down in the event of a disaster. The Superintendent and Board President told us they were not aware that the plan had not been updated. As a result, officials have no assurance that they would be able to protect data against loss or destruction and restore critical IT systems, applications or data timely in the event of a cyberattack or disaster.

Why Should Officials Provide IT Security Awareness Training?

To help minimize the risk of unauthorized access and misuse or loss of data and PPSI, school district officials should ensure periodic IT security awareness training is provided that explains rules of behavior for using the Internet and IT systems and data and communicates related policies and procedures to all employees. The training could center on, but not be limited to, emerging trends such as information theft and social engineering attacks (methods used to deceive users into revealing confidential or sensitive information), computer viruses and other types of malicious software, all of which may result in PPSI compromise. Training programs should be directed at the specific audience (i.e., system users or administrators).

The training should also cover key security concepts such as the dangers of downloading files and programs from the Internet or portable devices, such as thumb drives; the importance of selecting strong passwords; requirements related to protecting PPSI; risks involved with using unsecured Wi-Fi connections; or how to respond if a virus or an information security breach is detected.

…[D]istrict officials should ensure periodic IT security awareness training is provided that explains rules of behavior for using the Internet and IT systems and data. ...

Employees Were Not Provided Adequate IT Security Awareness Training

Officials did not ensure users were provided with comprehensive IT security awareness training to help ensure they understood IT security measures. Instead, the Assistant Superintendent and a former teacher appointed as the Data Privacy Officer told us staff received a brief training on phishing at the start of the 2021-22 school year. The training was provided by employees of one of the IT vendors. No other security topics were covered.

In conjunction with the training, staff are periodically sent phishing emails that provide staff with a short training video if they interact with the email, including opening the email or associated attachments. However, staff are not required to complete the training and are only sent reminder emails that a training is available for them. During our audit period, 161 staff members were sent these test phishing emails. Furthermore, 88 of the 161 employees that failed the exercise did not complete the training video. Fifty-three of those staff failed the training exercise more than once.

While the District's IT policies include some basic guidelines, and the IT vendor is responsible for providing annual IT training, the District does not have a written policy requiring all users to be trained in proper usage of the IT infrastructure, software and data. As a result, the District's IT assets and data are more vulnerable to loss and misuse, and employees may not be prepared to recognize and appropriately respond to suspicious system activity.

What Do We Recommend?

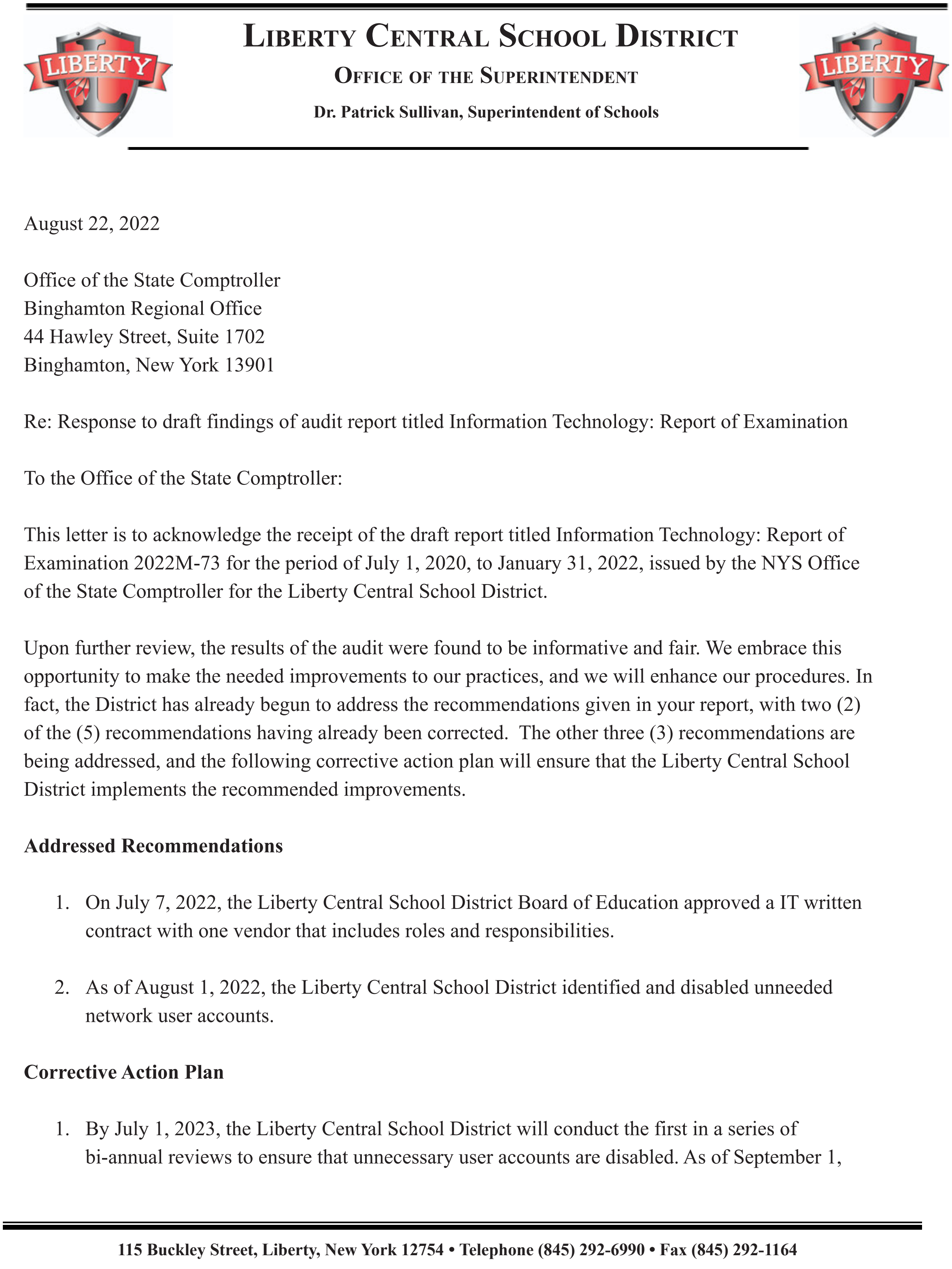
District officials should:

1. Develop comprehensive procedures for regularly reviewing user accounts and disabling those that are unnecessary.
2. Disable the identified unneeded network user accounts.
3. Ensure that periodic IT security awareness training is provided to personnel who use IT resources, including the importance of protecting PPSI and restricting physical access to systems and resources.
4. Ensure that the IT contingency plan is periodically reviewed and updated based on organizational or network changes with the District.

The Board should:

5. Ensure there is an adequate written IT contract and separate comprehensive written SLA with each vendor for IT services that will help ensure the District has an understanding of all services to be provided and the roles and responsibilities of the parties.

Appendix A: Response From District Officials



Liberty Central School District

Office of the Superintendent

Dr. Patrick Sullivan, Superintendent of Schools

August 22, 2022

Office of the State Comptroller
Binghamton Regional Office
44 Hawley Street, Suite 1702
Binghamton, New York 13901

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

To the Office of the State Comptroller:

This letter is to acknowledge the receipt of the draft report titled Information Technology: Report of Examination 2022M-73 for the period of July 1, 2020, to January 31, 2022, issued by the NYS Office of the State Comptroller for the Liberty Central School District.

Upon further review, the results of the audit were found to be informative and fair. We embrace this opportunity to make the needed improvements to our practices, and we will enhance our procedures. In fact, the District has already begun to address the recommendations given in your report, with two (2) of the (5) recommendations having already been corrected. The other three (3) recommendations are being addressed, and the following corrective action plan will ensure that the Liberty Central School District implements the recommended improvements.

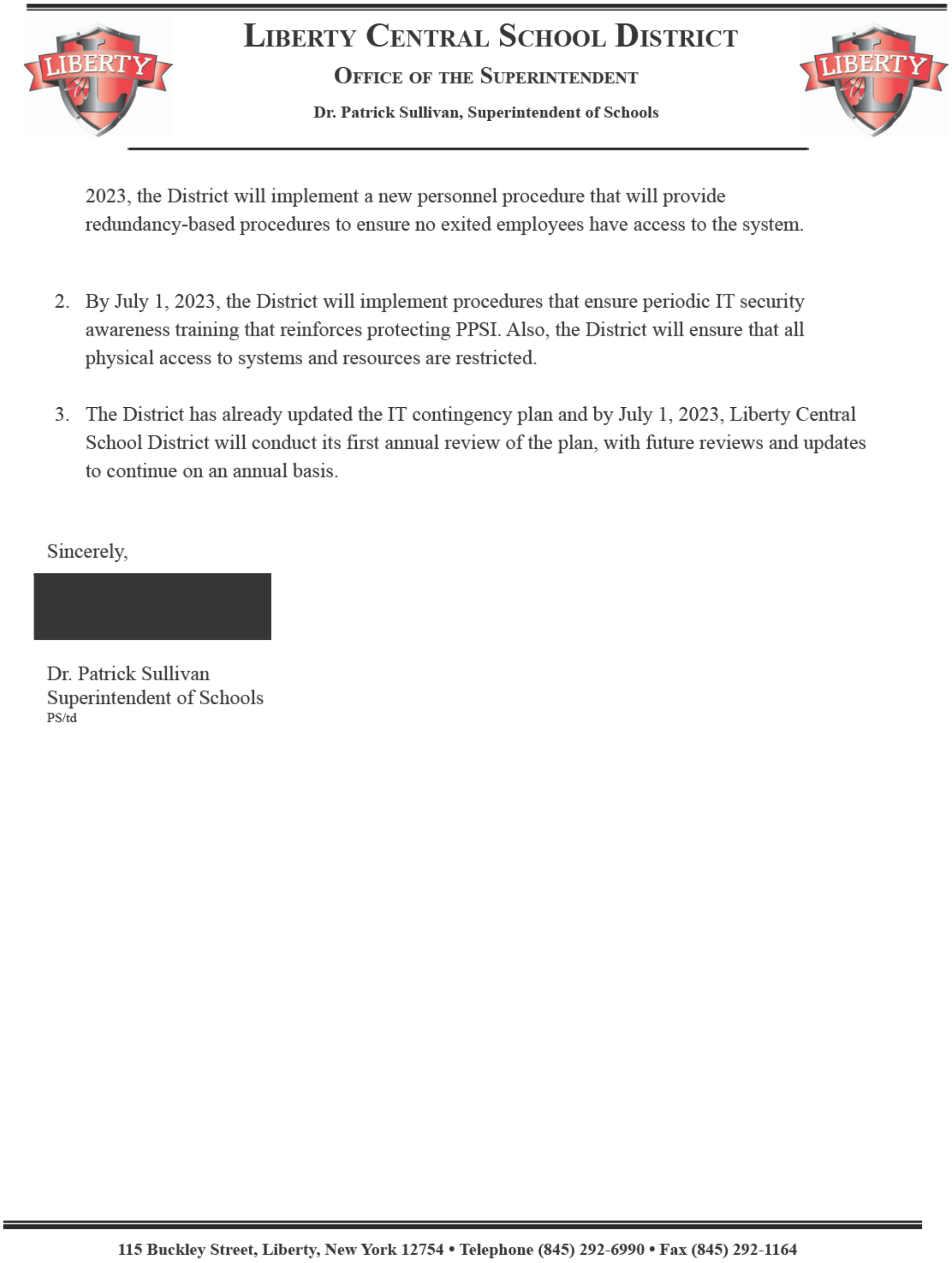
Addressed Recommendations

1. On July 7, 2022, the Liberty Central School District Board of Education approved a IT written contract with one vendor that includes roles and responsibilities.

2. As of August 1, 2022, the Liberty Central School District identified and disabled unneeded network user accounts.

Corrective Action Plan

1. By July 1, 2023, the Liberty Central School District will conduct the first in a series of bi-annual reviews to ensure that unnecessary user accounts are disabled. As of September 1,



2023, the District will implement a new personnel procedure that will provide redundancy-based procedures to ensure no exited employees have access to the system.

2. By July 1, 2023, the District will implement procedures that ensure periodic IT security awareness training that reinforces protecting PPSI. Also, the District will ensure that all physical access to systems and resources are restricted.

3. The District has already updated the IT contingency plan and by July 1, 2023, Liberty Central School District will conduct its first annual review of the plan, with future reviews and updates to continue on an annual basis.

Sincerely,

[redacted]

Dr. Patrick Sullivan
Superintendent of Schools
PS/td

Appendix B: Audit Methodology and Standards

We conducted this audit 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. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We interviewed District officials and IT vendor staff to obtain an understanding of the District's IT operations including the safeguards to protect sensitive data, the existence of an IT contingency plan and whether any employees received IT security awareness training.
- We used computerized audit scripts run on November 10, 2021 to analyze the District's network information about users (administrative and teacher/ student) to determine whether user accounts and security settings were necessary and appropriate. We reviewed user accounts and compared them to a list of current employees to identify potentially inactive and unneeded accounts. We also analyzed security settings and compared them to current industry standards to identify any inconsistencies.
- We reviewed contractual documents the District has with its IT vendors to determine the scope of IT services, reporting requirements, performance indicators and security procedures.

Our audit also examined the adequacy of certain IT controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to District officials.

We conducted this performance audit in accordance with generally accepted government auditing standards (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.

The Board has the responsibility to initiate corrective action. 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, 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. 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 CAP should be posted on the District's website for public review.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/files/local-government/publications/pdf/cyber-security-guide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/local-government/publications

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/local-government/academy

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

www.osc.state.ny.us/local-government

Local Government and School Accountability Help Line: (866) 321-8503

BINGHAMTON REGIONAL OFFICE – Ann C. Singer, Chief Examiner

State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417

Tel (607) 721-8306 • Fax (607) 721-8313 • Email: Muni-Binghamton@osc.ny.gov

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

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller