DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2019M-172

Geneseo Central School District

Online Banking

DECEMBER 2019

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

Contents

Report Highlights

Geneseo Central School District

Audit Objective

Determine whether District officials ensured online banking transactions were appropriate and secure.

Key Findings

District officials did not:

- Follow the Board's online banking policy or develop procedures to adequately segregate online banking duties.
- Ensure that authorized access to online bank accounts was limited.
- Provide information technology (IT) security awareness training to employees.

In addition, sensitive IT control weaknesses were communicated confidentially to District officials.

Key Recommendations

- Enforce the online banking policy and develop procedures to adequately segregate online banking duties.
- Designate one computer to be used strictly for online banking transactions.
- Ensure that officials and employees receive adequate IT security awareness training.

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

Background

The Geneseo Central School District (District) serves the Towns of Geneseo, Groveland, Sparta and West Sparta, all in Livingston County.

The District is governed by a Board of Education (Board), which is composed of seven elected members.

The Business Administrator is responsible for reviewing and authorizing online banking transactions. The District Treasurer (Treasurer) initiates bank and wire transfers using online banking, and the payroll clerk initiates online banking payroll transactions. The District uses network resources to perform online banking transactions. The Technology Coordinator is responsible for managing the network's security and the data it contains.

Quick Facts	
Employees	350
Enrollment	850
2019-20 Appropriations	$21.2 Million
Bank Balance as of July 31, 2019	$5.8 Million

Audit Period

July 1, 2017 – August 6, 2019

Online Banking

Online banking provides a means of direct access to funds held in district accounts. Users can review current account balances and account information, including recent transactions, and transfer money between bank accounts and to external accounts. Because wire transfers of funds typically involve significant amounts of money, districts must control the processing of their wire transfers to help prevent unauthorized transfers from occurring. It is essential that district officials authorize transfers before they are initiated and establish procedures to ensure that staff are securely accessing banking websites to help reduce the risk of unauthorized transfers from both internal and external sources.

How Can Officials Reduce the Risk of Inappropriate Online Banking Transactions?

To safeguard cash assets, a board must adopt policies and procedures to properly monitor and control online banking transactions. A comprehensive written online banking policy clearly describes the online activities district officials will engage in, specifies which employees are authorized to process transactions and establishes a detailed approval process to verify the accuracy and legitimacy of transfer requests. Officials must properly segregate the duties of employees granted access to the online banking applications to ensure that employees are unable to perform all financial transactions on their own. It is also essential that bank accounts be monitored by someone independent of the transaction for unauthorized or suspicious activity at least every two or three days.

Good management practices require limiting the number of users authorized to execute online banking activities and the number of computers used. Authorized online banking users should access bank accounts from one computer dedicated for online banking transactions. This will minimize exposure to malicious software because a dedicated computer could be used for isolated internet connections, be locked up after each use, and be hardwired rather than wireless. With the increased security protections afforded by a dedicated computer, transactions executed from those computers could be less at risk.

An acceptable use policy should inform users about appropriate and safe computer use. The District's acceptable use policy prescribes the development of regulations for computer use. Officials have adopted regulations that greatly detail acceptable and unacceptable use. Specifically, the regulations state that District computers are provided for educational purposes only. The regulations prohibit the wasteful use of these resources.

Officials Did Not Safeguard Online Banking Transactions

While the Board adopted an online banking policy, it did not specify which employees are authorized to process transactions. The policy also did not establish a detailed approval process to verify the accuracy and legitimacy of transfer requests. Officials did not adequately segregate online banking duties and ensure that authorized access to online bank accounts was limited. In addition, a dedicated separate computer was not used for these transactions and personal computer use was not limited, as discussed in the section regarding security awareness training.

The Business Administrator, Treasurer and payroll clerk each have their own username, password and security token[1] when making online transactions. The Treasurer initiates transfers between the District's bank accounts and wire transfers, while the payroll clerk initiates automated clearing house (ACH) debits for payroll. The Business Administrator has access to all the online banking abilities but does not initiate online banking transactions. Instead, he used it to get account notifications, such as low balances.

The use of the token limited unauthorized access from outside sources. However, both these individuals performed online banking transactions with no oversight because officials did not establish adequate security controls with the bank that required secondary authorizations for online transfers, wire transfers and ACH debits.[2] In addition, the Treasurer's and payroll clerk's computers and tokens were unsecured and accessible for anyone in the Business Office on multiple occasions.

The Treasurer received the bank statements, prepared bank reconciliations and regularly monitored activity for all accounts that she also performed online banking transactions for. The Treasurer compiles all pertinent online banking documentation as a part of the bank reconciliation and provides it to the Business Administrator for review up to a month after the online banking transactions occurred. As a result, District officials do not have an independent review designed to detect inappropriate online activity, and such transactions could go undetected and remain uncorrected.

We reviewed two months of online banking, wire transfer and ACH transactions, which included 117 transactions totaling $9.1 million. We found that all of these transactions were for appropriate purposes.

While we found no discrepancies in the transactions reviewed, without a sufficient policy that explicitly conveys practices to safeguard District assets during online banking transactions and the appropriate use of IT equipment, District officials cannot ensure that employees are aware of their responsibilities. Further, the lack of a dedicated online banking computer could result in users unintentionally exposing the online bank accounts to threats from malicious software, which could subject cash assets to misappropriation.

[1] Token identifications contain a number series assigned to a specific user.

[2] Online debt service payments required secondary approval by the Business Administrator.

Why Should the District Provide IT Security Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data and personal, private and sensitive information (PPSI), district officials should provide periodic IT security awareness training that explains the proper rules of behavior for using the Internet and IT systems and data and communicates related policies and procedures to all employees and students. The training should center on emerging trends such as information theft, social engineering attacks[3] and 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 (e.g., system users or administrators) and include everything that attendees need to perform their jobs.

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.

District Employees Were Not Provided With IT Security Awareness Training

The District's acceptable use policy and regulations provide detailed guidelines for using District IT assets and explicitly state that IT assets are provided solely for educational purposes and research consistent with the District's missions and goals. However, the District did not provide users with IT security awareness training to help ensure they understood IT security measures. The IT cybersecurity community identifies people as the weakest link in the chain to secure data and IT systems. District officials cannot protect the confidentiality, integrity and availability of data and computer systems without ensuring that users, or those who manage IT, understand the IT security policies and procedures and their roles and responsibilities related to IT and data security. Without periodic, formal IT security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise IT assets. As a result, data and PPSI could be at greater risk for unauthorized access, misuse or abuse.

Because officials did not provide IT security awareness training or enforce the District's acceptable use policy prohibiting personal use of District computers, we reviewed the website browsing histories on the Business Administrator's, Treasurer's and payroll clerk's computers and identified questionable personal use on all of these computers. Users accessed websites for online shopping,

[3] Social engineering attacks are methods used to deceive users into revealing confidential or sensitive information.

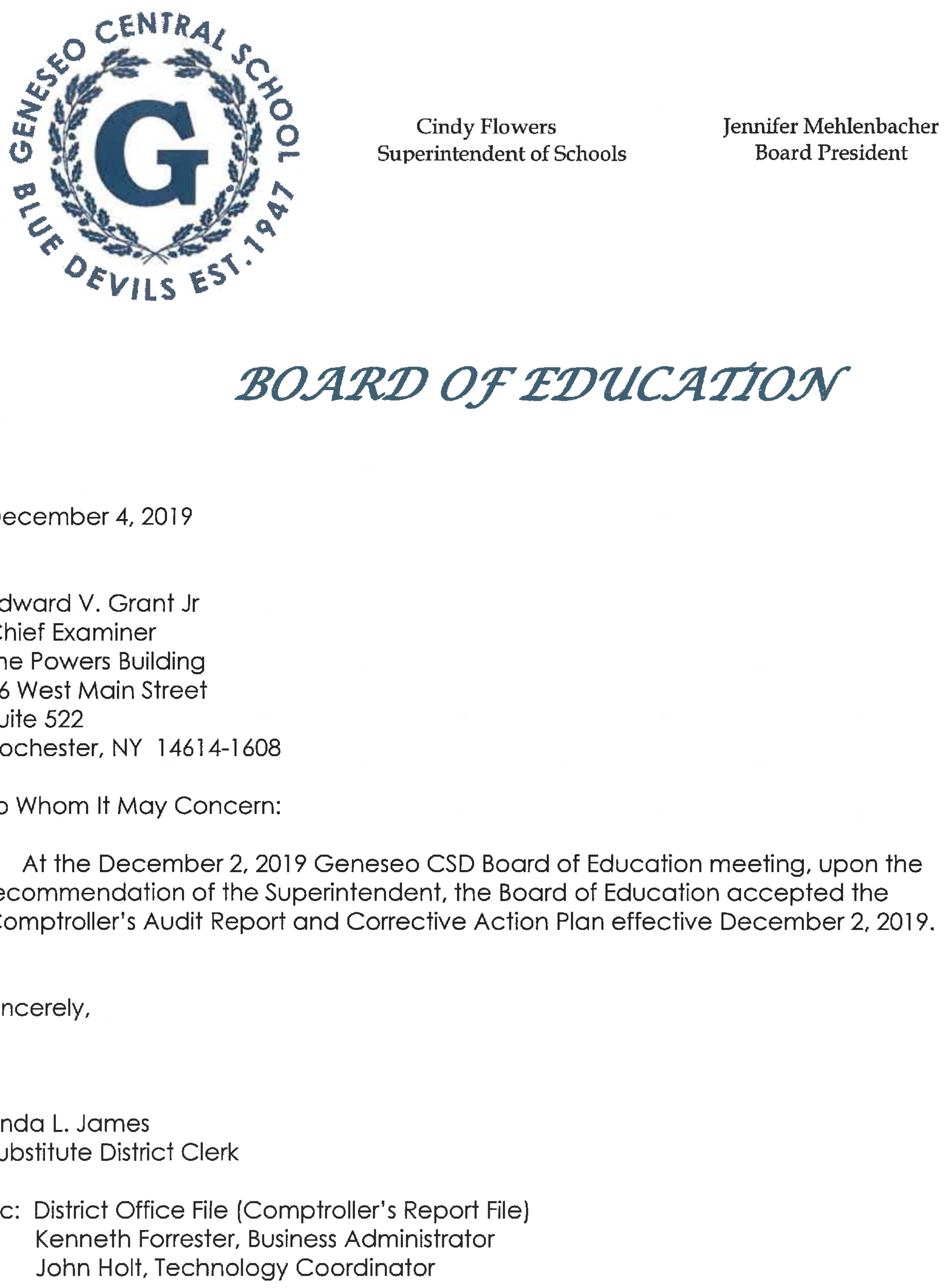
news and entertainment, radio and video streaming, and personal banking, which were not allowed per the District's acceptable use policy and regulations. Allowing personal use of computers increases the risk of malicious software and attacks on the computer system and can decrease employee productivity.

What Do We Recommend?

District officials should:

1. Develop procedures to adequately segregate online banking duties.
2. Enable notifications and other security measures available from the bank, including secondary approvals and email notifications every time an online transaction occurs.
3. Designate a computer to be used for online banking transactions.
4. Provide periodic IT security awareness training that reflects current risks identified by the IT cybersecurity community to personnel who use IT resources.
5. Monitor computer use to ensure compliance with the acceptable use policy and regulations.

Appendix A: Response From District Officials



GENESEO CENTRAL SCHOOL BLUE DEVILS EST. 1947

Cindy Flowers
Superintendent of Schools

Jennifer Mehlenbacher
Board President

BOARD OF EDUCATION

December 4, 2019

Edward V. Grant Jr
Chief Examiner
The Powers Building
16 West Main Street
Suite 522
Rochester, NY 14614-1608

To Whom It May Concern:

At the December 2, 2019 Geneseo CSD Board of Education meeting, upon the recommendation of the Superintendent, the Board of Education accepted the Comptroller's Audit Report and Corrective Action Plan effective December 2, 2019.

Sincerely,

Linda L. James
Substitute District Clerk

cc: District Office File (Comptroller's Report File)
Kenneth Forrester, Business Administrator
John Holt, Technology Coordinator

Geneseo Central School District

4050 Avon Road
Geneseo, NY 14454
At David Dwyer Way

Cindy Flowers
Superintendent

Jennifer Mehlenbacher
Board President

Telephone: 585.243.3450
Fax: 585.243.9481

Response From Geneseo Central School District Regarding NYS Comptroller Audit Presented in November, 2019

November 22, 2019

Edward V. Grant Jr
Chief Examiner
Division of Local Government and School Accountability
Office of the New York State Comptroller

Dear Mr. Grant:

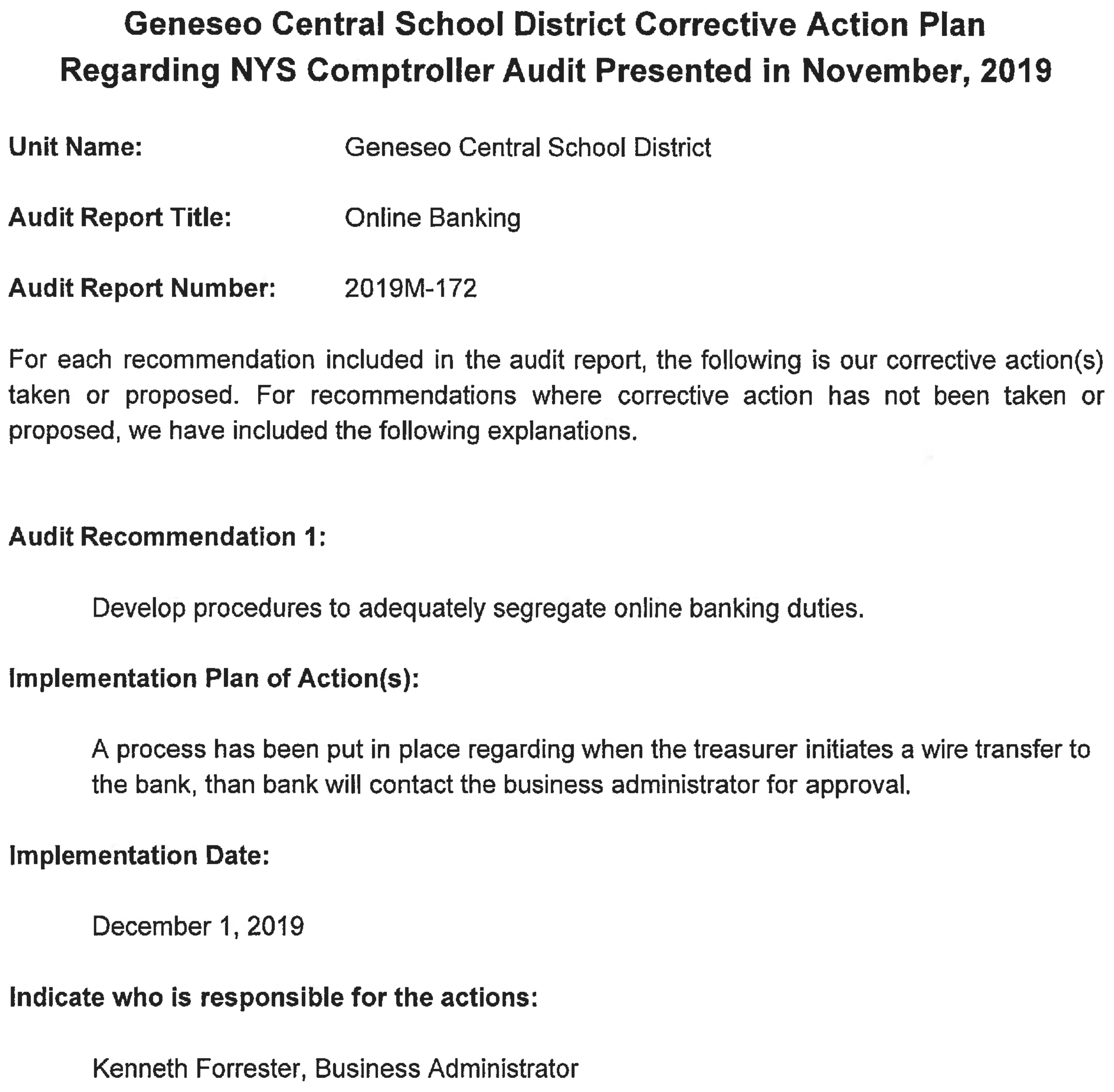
Thank you for providing our district with the findings regarding the Online Banking and IT Audit that your office coordinated. This letter is to inform you that we are combining our response and our Corrective Action Plan into one document.

We agree with the findings in your audit and appreciate the recommendations that you have given to our district. Many of the recommendations have already been implemented in the district and changes have begun to be made based on these recommendations.

Please review our Corrective Action Plan and feel free to contact us if you have any questions regarding these plans.

Sincerely,

Cindy Flowers
Superintendent of Schools



Geneseo Central School District Corrective Action Plan Regarding NYS Comptroller Audit Presented in November, 2019

Unit Name:	Geneseo Central School District
Audit Report Title:	Online Banking
Audit Report Number:	2019M-172

For each recommendation included in the audit report, the following is our corrective action(s) taken or proposed. For recommendations where corrective action has not been taken or proposed, we have included the following explanations.

Audit Recommendation 1:

Develop procedures to adequately segregate online banking duties.

Implementation Plan of Action(s):

A process has been put in place regarding when the treasurer initiates a wire transfer to the bank, than bank will contact the business administrator for approval.

Implementation Date:

December 1, 2019

Indicate who is responsible for the actions:

Kenneth Forrester, Business Administrator

Audit Recommendation 2:

Enable notifications and other security measures available from the bank, including secondary approvals and email notifications every time an online transaction occurs.

Implementation Plan of Action(s):

The bank will send email notifications to the business administrator anytime online transactions occur. The Board Policy (5510) will be updated to reflect identification of which employees can initiate online transactions (Treasurer, Payroll Clerk, and Business Administrator).

Implementation Date:

December 1, 2019

Indicate who is responsible for the actions:

Kenneth Forrester, Business Administrator

Audit Recommendation 3:

Designate a computer to be used for online banking transactions.

Implementation Plan of Action(s):

A laptop has been designated to be used by the business office for online banking transactions. Only the three members of the business office (Business Administrator, Treasurer, Payroll Clerk) can login to this laptop and their user profiles will be deleted after every use ensuring that passwords and browsing history are removed. When the laptop is not being used, the device will be in a secure location in the business office.

Implementation Date:

December 1, 2019

Indicate who is responsible for the actions:

John Holt, Technology Coordinator

Audit Recommendation 4:

Provide periodic IT security awareness training that reflects current risks identified by the IT cybersecurity community to personnel who use IT resources.

Implementation Plan of Action(s):

Every staff member must complete a Safeschools Online Training which is a cybersecurity risk training, focused primarily on risks associated with email malware attacks.

Implementation Date:

September 1, 2019

Indicate who is responsible for the actions:

John Holt, Technology Coordinator

Audit Recommendation 5:

Monitor computer use to ensure compliance with the acceptable use policy and regulations.

Implementation Plan of Action(s):

Periodic scans of computer use to ensure compliance with district Acceptable Use Policy regarding personal website usage. This can be accomplished through our iBoss Internet Filtering reporting.

Implementation Date:

December 1, 2019

Indicate who is responsible for the actions:

John Holt, Technology Coordinator

IT Audit Recommendation(s):

Recommendations were made internally to our IT Department regarding usernames, remote access to computers, password requirements, administrative accounts, third party patch management for software, and policies regarding locking screens.

Implementation Plan of Action(s):

The recommendations presented to our IT Department have resulted in the adjustment of computer policies and removal of potentially targeted accounts noted in the audit.

Implementation Date:

December 1, 2019

Indicate who is responsible for the actions:

John Holt, Technology Coordinator

Signed:

Name Cindy Flowers

Date 12/2/19

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 to obtain an understanding of online banking practices and to obtain any related policies and procedures.
- We reviewed policies and procedures for acceptable use of IT.
- We observed online banking users' access from logon to logoff for the Business Administrator, Treasurer and payroll clerk.
- We inquired about a written agreement with the bank and reviewed the documentation regarding capabilities for electronic transfers.
- We examined the three computers for users that had access to online banking.
- We reviewed all online banking transactions for two months to determine whether they were appropriate District expenditures. We randomly selected the months of February and April 2019.

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 GAGAS (generally accepted government auditing standards). 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.

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 2116-1(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 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. We encourage the Board to make the CAP available for public review in the Clerk's office.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/localgov/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/localgov/costsavings/index.htm

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/localgov/fiscalmonitoring/index.htm

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/localgov/pubs/listacctg.htm#lgmg

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/localgov/planbudget/index.htm

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/localgov/pubs/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/localgov/finreporting/index.htm

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/localgov/researchpubs/index.htm

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

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/localgov/index.htm

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

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief Examiner

The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608

Tel (585) 454-2460 • Fax (585) 454-3545 • Email: Muni-Rochester@osc.ny.gov

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

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