DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2020M-118

Cayuga County Soil and Water Conservation District

Information Technology Governance

NOVEMBER 2020

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

Cayuga County Soil and Water Conservation District

Audit Objective

Determine whether Cayuga County Soil and Water Conservation District (District) officials adequately safeguarded information technology (IT) assets.

Key Findings

District officials did not establish adequate controls over IT assets. The Board did not:

- Develop comprehensive IT policies or procedures.
- Enter into a written service level agreement (SLA) with the IT vendor.
- Establish adequate safeguards for online banking transactions.
- Implement strong access and financial application controls.
- Provide IT security awareness training for employees who use District IT assets.

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

Key Recommendations

The Board should:

- Adopt comprehensive IT security policies and periodically review them.
- Enter into a SLA with the IT vendor.
- Provide IT security awareness training to personnel who use IT assets.

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

Background

The District is located in Cayuga County (County) and is a component unit of the County. The District provides services to improve and maintain wildlife habitat, help control and prevent water pollution and manage erosion control and other related land use issues.

The District is governed by a seven-member appointed Board of Directors (Board). The Executive Director is responsible for managing the District's day-to-day operations under the Board's direction.

The District relies on its IT system for Internet access, email, maintaining financial data, and maintaining and accessing personal, private or sensitive information (PPSI). District officials relied on an IT vendor for IT services and technical assistance, as needed.

Quick Facts	
2019 Budget	$3.1 million
Employees	13
Computers	18
Server	1

Audit Period

January 1, 2018 – April 10, 2020

Information Technology (IT)

What Policies and Procedures Should the Board Adopt to Safeguard District IT Assets?

IT security policies describe the tools and procedures to protect data and information systems, define appropriate user behavior and explain the consequences of policy violations. Therefore, it is essential for the board to establish security policies for key IT security issues.

The board should have acceptable computer use policies that define specific consequences for violations and address security awareness. Additionally, the board should establish computer policies that take into account people, processes and technology and communicate them throughout the district.[1] New York State Technology Law requires municipalities and other local agencies to have a breach notification policy that requires notification be given to certain individuals in the event of a system security breach, as it relates to private information. Finally, the board should periodically review these policies, update them as needed and stipulate who is responsible for monitoring IT policies.

IT vendors and employees did not have guidance related to the appropriate use of District IT assets.

The Board Did Not Adopt IT Security Policies and Procedures

The Board did not adopt IT security policies and procedures addressing key IT security issues, such as those related to acceptable use, online banking, sanitation and disposal of IT equipment, password security, mobile computing and storage devices, wireless networks, use and access of PPSI and breach notification. The Board also has not adopted a comprehensive disaster recovery plan. Therefore, IT vendors and employees did not have guidance related to the appropriate use of District IT assets. Consequently, IT assets are at risk for unauthorized, inappropriate and wasteful use, and the District could incur a potentially costly disruption of operations and services.

While IT policies will not guarantee the safety of the District's systems, a lack of appropriate policies significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate use or access. Without formal policies that explicitly convey the appropriate use of the District's computer equipment and practices to safeguard data, officials cannot ensure that employees are aware of their responsibilities.

What Should Be Included In an IT Vendor Contract?

District officials must ensure that they have qualified IT personnel to manage the district's IT environment. This can be accomplished by using district employees, an IT service provider (IT vendor) or both. To avoid potential misunderstandings

[1] Refer to our publication *Information Technology Governance* available at http://www.osc.state.ny.us/localgov/pubs/lgmg/itgovernance.pdf

and to protect district assets, the district should have a written agreement with its IT vendor that clearly states the district's needs and service expectations. The agreement must include provisions relating to confidentiality and protection of personal, private and sensitive data and specify the level of service to be provided.

The Board Did Not Contract with the IT Vendor

District officials relied on an IT vendor for IT services and technical assistance, as needed. The Board does not have a written service level agreement (SLA) with its IT vendor that identifies the District's needs and expectations and specifies the level of service to be provided by the IT vendor.

The District buys blocks of time from its IT vendor at a specific price. The District uses these blocks of time for network support, routine maintenance and tape backup administration. The District paid its IT vendor $6,065 in 2018 without a formal contract.

Without an SLA, the roles and responsibilities of each party are not defined. The lack of a written agreement put the District's IT assets and data at greater risk for unauthorized access, misuse or loss.

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

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, the processing of district wire transfers must be controlled 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 employees are securely accessing banking websites to help reduce the risk of unauthorized transfers from both internal and external sources.

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. Segregation of duties should include monitoring bank accounts 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. Banking agreements should identify current authorized users, and authorized online banking users should access bank accounts from one computer dedicated for online banking transactions. This will minimize exposure to malicious software because the other computers are used for activities that may introduce additional risk to the computers' integrity, and transactions executed from those computers could be more at risk.

District Officials Did Not Safeguard Online Banking Transactions

Because the Board did not adopt an online banking policy and the bank agreement was inadequate, a detailed approval process to verify the accuracy and legitimacy of online banking transactions was not established. District officials did not adequately segregate online banking duties, ensure authorized access to bank accounts was limited, or maintain adequate banking agreements. Officials also did not use a dedicated separate computer for these transactions or prohibit personal use on computers used for online banking.

District officials did not adequately segregate online banking duties, ensure authorized access to bank accounts was limited, or maintain adequate banking agreements.

Three employees each have their own usernames and passwords when making online banking transactions. However, they all know each other's credentials, so individual accountability is not maintained. The first employee performs online banking transactions with no oversight because the District's outdated banking agreements did not establish adequate security controls, such as requiring secondary authorizations for online transfers and automated clearing house (ACH) transactions. This employee also initiates transfers between the District's bank accounts and initiates ACH transactions on the same computer that she performs all her other duties and Internet browsing. The second employee has access to all online banking abilities but does not initiate online banking transactions. The third employee prepares bank reconciliations and accesses the online banking website to print bank statements and canceled checks, but cannot initiate transfers or ACH transactions.

We reviewed the month of August 2018 bank deposits and ACH transactions, which included 52 transactions totaling $714,015. We found these transactions were for appropriate District 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.

Why Should District Officials Provide IT Security Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data and 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. The training should center on emerging trends such as information theft, social engineering attacks[2] 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, such as secure online banking for users who perform online banking transactions.

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 Officials Did Not Provide IT Security Awareness Training To IT Users

District officials did not provide IT users with IT security awareness training to help ensure they understood IT security measures designed to safeguard online activity. 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 IT security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise the District's IT assets and security. As a result, online banking transactions, District financial data and PPSI could be at a greater risk for unauthorized access, misuse or abuse.

The website browsing histories on 12 of the 18 District computers identified questionable personal use on all of them.

Because District officials and employees were not provided IT security awareness training, we reviewed the website browsing histories on 12 of the 18 District computers and identified questionable personal use on all of them. District employees visited websites that were potentially for non-business purposes, and performed other Internet research and browsing of a personal nature using the District's IT assets. District employees visited social networking, online shopping,

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

bill pay, healthcare, banking, travel, education, sports, job searching, investment and other financial websites, personal email, video and music streaming and other entertainment websites. Because the Board has not adopted an acceptable use policy, we were unable to determine whether these actions were allowable. However, not prohibiting personal use of computers increases the risk of malicious software and attacks on the computer system and can decrease employee productivity.

What Are Strong Access Controls?

District officials are responsible for restricting users' access to just those applications, resources and data that are necessary for their day-to-day learning, duties and responsibilities to provide reasonable assurance that computer resources are protected from unauthorized use or modifications. User accounts enable the system to recognize specific users, grant the appropriately authorized access rights and provide user accountability by affiliating user accounts with specific users, not sharing user accounts among multiple users and disabling generic user accounts. Users with administrative rights and remote access must also be limited and all user access should be monitored. Finally, all users should set their own passwords within prescribed requirements. Holding passwords to certain complexity, length and age requirements makes passwords more difficult to crack or be easily guessed.

We observed employees logging into computers with other users' IDs and passwords.

To help ensure individual accountability within the network and software applications, each user should have his or her own network and software applications accounts (username and password). If users share accounts, accountability is diminished and activity in the system may not be able to be traced back to a single user.

Officials Did Not Enable Strong Access Controls

District officials have not implemented comprehensive procedures for managing, limiting, securing and monitoring user access. As a result, we noted inactive user accounts and excessive administrator user accounts.

Specifically, 17 of the 35 network user accounts (49 percent) have not been used in the last six months and four user accounts (11 percent) were for individuals no longer employed at the District. Consequently, the District's IT assets and data are at increased risk for loss or misuse. We also identified 20 generic network user accounts which were unnecessary. In addition, we observed employees logging into computers with other users' IDs and passwords. Because generic accounts are used and multiple users share user account credentials, any suspicious activity could not be traced to a single user. Consequently, the District's IT assets are at increased risk for loss or misuse.

What Are Effective Application Controls?

Officials should segregate duties within the financial application to ensure that employees are granted access needed to perform their duties, but cannot perform all phases of a transaction. Additionally, audit logs should be reviewed to ensure individuals are making only authorized changes in the application. Any unusual or unauthorized activity could indicate a breakdown in controls or possible malfeasance.

District officials did not adequately segregate duties within the financial application or implement mitigating controls.

District Officials Did Not Implement Strong Financial Application Controls

We reviewed users' financial application permissions and found District officials did not adequately segregate duties within the financial application or implement mitigating controls. The Clerk prepares and makes deposits, records and reports all money received and disbursed, and makes any adjusting entries in the financial accounting software. In addition, the Clerk is the administrator of the financial application and is responsible for adding, deleting or modifying user accounts and their access rights with limited oversight. Although the senior typist reviews all disbursements for proper approval and recording prior to mailing the checks and the Executive Director reviews bank statements and reconciliations, audit logs and journal entries are not printed or reviewed from the financial accounting software.

We found the access rights assigned to the senior typist were adequate for her job responsibilities. However, the nutrient management specialist has full user permissions that allow him to make adjustments, transfer funds, and modify and delete transactions. District officials were not aware of these user permissions and agreed this level of access was not necessary for his job responsibilities of monitoring grant revenues and expenditures.

We reviewed 52 receipts totaling $714,015 and 27 payments totaling $11,118 from the month of August 2018 and found all were properly recorded. Additionally, we reviewed all State grant funding for 2018 totaling approximately $1.8 million and found they were properly recorded.

Although we did not find any discrepancies, granting users excessive permissions increase the risk that they could initiate improper transactions without detection.

What Do We Recommend?

The Board and District officials should:

1. Adopt comprehensive IT security policies addressing acceptable use, online banking, sanitation and disposal of IT equipment, password

security, mobile computing and storage devices, wireless networks, use of and access to PPSI and breach notification.

2. Periodically review and update all IT policies and procedures to reflect changes in technology and the District’s computing environment and designate personnel who are responsible for monitoring all IT policies.

3. Develop and adopt a comprehensive written disaster recovery plan and ensure it is distributed to all responsible parties, periodically tested and updated as needed. Also, ensure data backups are periodically tested.

4. Enter into an SLA with the IT vendor that sufficiently defines the role and responsibilities of each party, includes all services to be provided, and addresses confidentiality and protection of PPSI.

5. Ensure banking agreements reflect current operations and provide for adequate controls over online banking transactions.

6. Develop procedures to adequately segregate online banking duties.

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

8. Designate a computer to be used for online banking transactions.

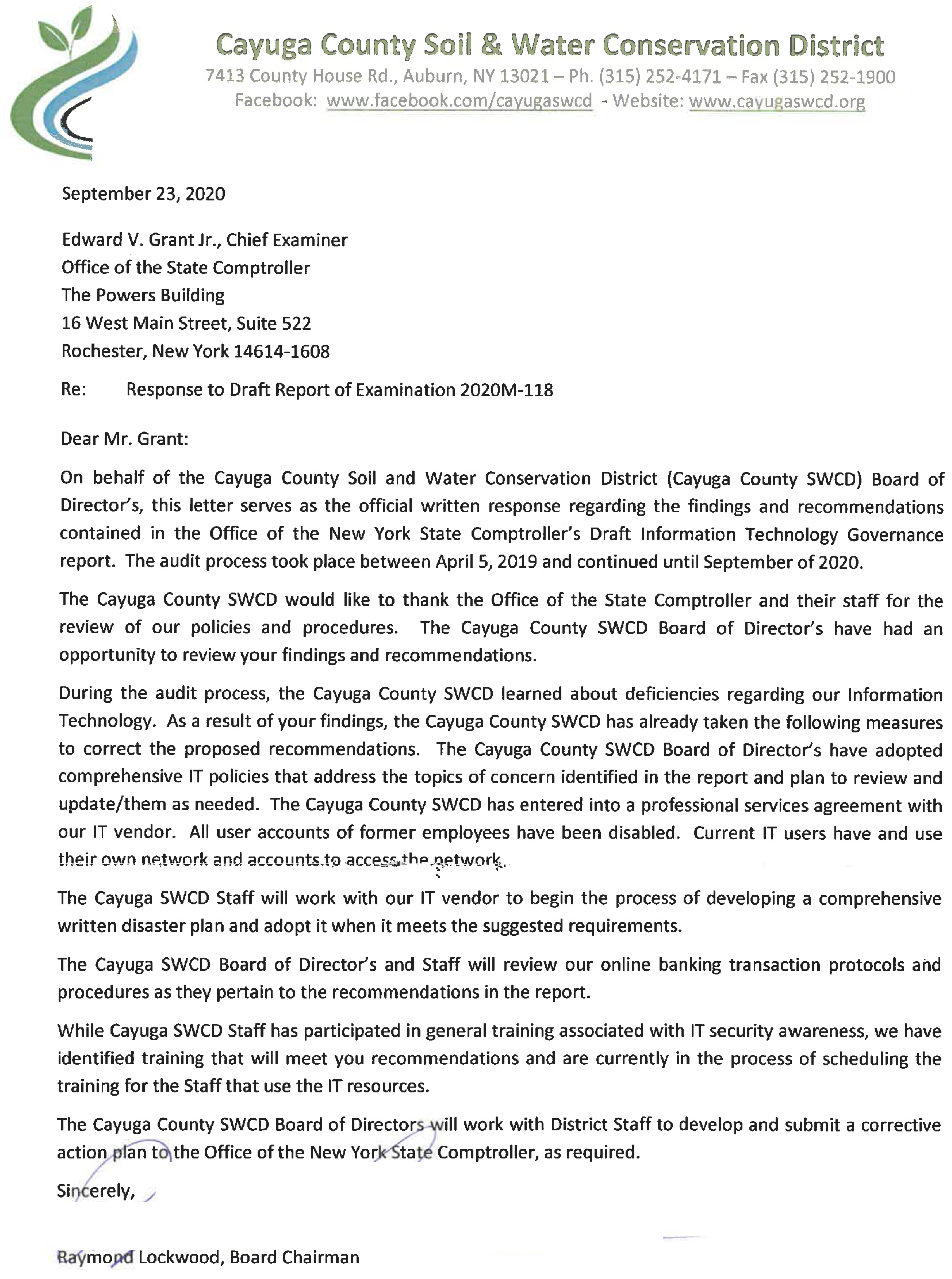
9. Provide periodic IT security awareness training to District officials and employees who use IT resources, including the importance of physical security and protection of PPSI.

10. Immediately disable user accounts of former employees and regularly review and update user accounts for necessity and appropriateness.

11. Ensure all IT users have and use their own network and application user accounts to access the network and specialized software applications, where necessary.

12. Assess user permissions for all network and application user accounts on a regular basis and remove excessive user permissions for those users who do not need that level of access to perform their job duties.

Appendix A: Response From District Officials



Cayuga County Soil & Water Conservation District
7413 County House Rd., Auburn, NY 13021 – Ph. (315) 252-4171 – Fax (315) 252-1900
Facebook: www.facebook.com/cayugaswcd - Website: www.cayugaswcd.org

September 23, 2020

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

Re: Response to Draft Report of Examination 2020M-118

Dear Mr. Grant:

On behalf of the Cayuga County Soil and Water Conservation District (Cayuga County SWCD) Board of Director's, this letter serves as the official written response regarding the findings and recommendations contained in the Office of the New York State Comptroller's Draft Information Technology Governance report. The audit process took place between April 5, 2019 and continued until September of 2020.

The Cayuga County SWCD would like to thank the Office of the State Comptroller and their staff for the review of our policies and procedures. The Cayuga County SWCD Board of Director's have had an opportunity to review your findings and recommendations.

During the audit process, the Cayuga County SWCD learned about deficiencies regarding our Information Technology. As a result of your findings, the Cayuga County SWCD has already taken the following measures to correct the proposed recommendations. The Cayuga County SWCD Board of Director's have adopted comprehensive IT policies that address the topics of concern identified in the report and plan to review and update/them as needed. The Cayuga County SWCD has entered into a professional services agreement with our IT vendor. All user accounts of former employees have been disabled. Current IT users have and use their own network and accounts to access the network.

The Cayuga SWCD Staff will work with our IT vendor to begin the process of developing a comprehensive written disaster plan and adopt it when it meets the suggested requirements.

The Cayuga SWCD Board of Director's and Staff will review our online banking transaction protocols and procedures as they pertain to the recommendations in the report.

While Cayuga SWCD Staff has participated in general training associated with IT security awareness, we have identified training that will meet you recommendations and are currently in the process of scheduling the training for the Staff that use the IT resources.

The Cayuga County SWCD Board of Directors will work with District Staff to develop and submit a corrective action plan to the Office of the New York State Comptroller, as required.

Sincerely,

Raymond Lockwood, Board Chairman

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[3] and obtain valid audit evidence, our audit procedures included the following:

- We interviewed District officials and reviewed the Board minutes, resolutions and District policies to gain an understanding of the District's controls over IT assets.
- We inquired about IT policies and procedures.
- We interviewed the IT consultant to gain an understanding of the District's IT environment. Additionally, we reviewed the District's invoices for IT services.
- We reviewed the District's inventory to determine whether it was adequate and performed a physical inventory of computers on site to determine whether all District computers were properly recorded on the inventory.
- We used our professional judgment to select a sample of 12 computers and ran a specialized computer audit tool on the server and 11 operational District computers. We used the tool to identify installed software, local account password settings and user account configurations.
- We manually reviewed four computers for installed software, local account settings and user account configurations.
- We reviewed Internet history on the server and all 11 operational computers to determine whether the computers were being used for appropriate business activities.
- We compared system users to payroll reports to determine whether users were currently employed by the District.

Our audit also examined the adequacy of certain information technology 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.

[3] We also issued a separate report, *Cayuga County Soil and Water Conservation District, Financial Condition* (2020M-91).

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.

A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law. 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/sites/default/files/local-government/documents/pdf/2018-12/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263196&issued=All

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?title=&body_value=&field_topics_target_id=263206&issued=All

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/sites/default/files/local-government/documents/pdf/2020-05/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?title=&body_value=&field_topics_target_id=263211&issued=All

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

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