DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2020M-33

Town of Westerlo

Information Technology

JUNE 2020

OFFICE OF THE NEW YORK STATE COMPTROLLER

Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

Town of Westerlo

Audit Objective

Determine whether Town officials adequately safeguarded information technology (IT) resources.

Key Findings

Town officials have not:

- Established appropriate policies and procedures to safeguard IT resources.
- Implemented strong access controls over user accounts and have not disabled unnecessary accounts.
- Formalized a contract describing specific services to be provided by the Town's third-party IT vendor.

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

Key Recommendations

- Adopt policies and procedures for safeguarding IT resources.
- Implement strong access controls, in part, by disabling unnecessary user accounts.
- Develop a service level agreement with the third-party vendor to address the Town's specific needs and expectations for IT services.

Town officials generally agreed with our recommendations and have initiated, or indicated they planned to initiate, corrective action.

Background

The Town of Westerlo (Town) is located in Albany County. The Town is governed by an elected Town Board (Board) composed of a Town Supervisor and four Board members. The Board is responsible for the general oversight of operations and finances, including security over the Town's IT system.

Town officials contract with a third-party vendor for IT services including support, network management and other services.

Quick Facts	
Residents	3,455
2019 General Fund Budget	$3 million
Employees	54
Network Accounts	12

Audit Period

January 1, 2018 – September 30, 2019. We extended the scope to November 6, 2019 for IT information collection.

Information Technology

The Town relies on its IT system for Internet and email access, as well as maintaining and accessing financial data and applications that reside within the network. Therefore, the IT system and data are valuable Town resources. If the IT system becomes compromised, the results could range from inconvenient to catastrophic and could require extensive effort and resources to evaluate and repair. While effective controls will not guarantee the safety of an IT system, the lack of effective controls significantly increase the risk that data, hardware and software may be lost or damaged by inappropriate access and use.

How Should IT Resources Be Safeguarded?

A board should establish computer policies that take into account people, processes and technology. Each town's unique computing environment should dictate the content and number of policies necessary. Computer policies can include information related to Internet, email and personal computer use; use of and access to personal, private and sensitive information (PPSI); password security; and information security management. It is also important for town officials to communicate policies to employees and to monitor compliance with policies.

As part of that communication, and to ensure the highest level of security over town data, town officials should adopt policies and procedures for information security management, including cybersecurity awareness training to inform employees of security risks and train them in practices that reduce internal and external threats to IT systems and data. While the IT policies tell computer users what to do, cybersecurity training provides them with the skills to do it. IT training should be directed at the specific audience (e.g., user or system administrator) and should include everything they need to perform their job duties.

Town officials are also responsible for restricting users' access to just those applications, resources and data that are necessary for their day-to-day duties to provide reasonable assurance that computer resources are protected from unauthorized use or modifications. User accounts enable the system to recognize specific users, grant appropriate authorized access rights and provide user accountability by affiliating user accounts with a specific user and not sharing user accounts with multiple users. In addition, accounts belonging to those who left town employment should be disabled. Town officials should develop written procedures for granting, changing and disabling user accounts to help ensure account access is applied consistently.

Due to the increasing reliance on third-parties to provide a variety of IT-related services, town officials should formalize this relationship. Written agreements should define the contractual relationship and responsibilities between the IT service provider and the town, including what services will be provided, when they will be provided, how they will be provided, and at what cost. A written agreement should also stipulate that the IT service provider will have a system of internal controls in place to provide reasonable assurance that the town's information will be protected against loss, abuse and fraudulent activity.

In addition, to protect the town and avoid potential misunderstandings, officials should have a written service level agreement (SLA) between the town and its third-party vendor (vendor) that identifies the town's needs and expectations and specifies the level of service to be provided by the vendor. An SLA is different from a traditional written contract in that it establishes comprehensive, measureable 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; duration of the agreement; scope and/or subject limitations; service level objectives and performance indicators; roles and responsibilities; nonperformance impact; security and audit procedures; reporting requirements; review, update and approval process; and pricing, billing and terms of payment.

Safeguarding IT assets should also include town officials developing and adopting a disaster recovery plan to anticipate and reconstruct vital operations and services after a disaster. Disasters may include any sudden, catastrophic event that compromises the availability or integrity of an IT system and data. Typically, a disaster recovery plan includes an analysis of business processes and continuity needs, disaster prevention instructions, specific roles of key individuals and precautions needed to maintain or quickly resume operations. Additionally, a disaster recovery plan should include data backup procedures such as requiring periodic backup testing to ensure they will function as expected.

Town Officials Have Not Developed and Communicated Adequate IT Policies

The Board has not adopted or implemented IT policies and procedures addressing acceptable computer use, access to PPSI, password security or information security management. Without policies and procedures, Town officials and employees may not be properly aware of how to safeguard IT resources. In addition, the Board did not provide users with security awareness training to help ensure they understood security measures needed to protect the network because the Board lacked sufficient knowledge and experience related to IT.

The failure to develop policies and procedures and provide IT security training to raise awareness increases the risk that users will not understand their responsibilities, putting the data and computer resources at greater risk for unauthorized access, misuse or abuse.

Town Officials Did Not Implement Strong Access Controls

Town officials have not implemented comprehensive procedures for managing, limiting, securing and monitoring user accounts. Town officials relied on a vendor for account maintenance but did not have a process in place to ensure strong access controls were implemented. Specifically, officials did not adequately communicate their needs with the vendor. As a result, access rights and permissions for network, local and financial application users were not properly granted based on job duties.

We reviewed the Town's 12 network user accounts[1] and found:

- Three accounts (25 percent) did not match current employees, and one of these accounts was not used in more than five years. These accounts belonged to prior Town employees who left Town employment one, eight and 10 months before our review, and the accounts have not been disabled.
- Five accounts (42 percent) also have local administrative permissions. The vendor indicated local administrative permissions are granted to reconnect or connect a computer to a group and to install updates for software applications. The misuse of administrative permissions is a method often used by attackers to compromise or disrupt systems.
- Two Deputy Town Clerks use the same credentials (i.e., one account) to access the network.
- The Town Clerk shares the password for her network credentials with the two Deputy Town Clerks.

We also reviewed 11 local user accounts[2] on the server and four user computers and found that three accounts (27 percent) have unnecessary administrative permissions. These users can unnecessarily make system-wide changes, including installing programs and manipulating settings configured for security purposes. Two of the accounts with unnecessary administrative permissions have not been used in more than five years and appear unnecessary.

We reviewed the accounts within the Town's financial application. We found that prior to August 2019, all four users shared a single administrative account, giving users unnecessary permissions. This also allowed the administrative account to be used for non-administrative tasks, creating a lack of accountability. On August 28, 2019, the vendor added three user accounts upon the Town's request. However, users continued to share accounts and access was not adequately

[1] Network user accounts are those accounts that are stored on a centralized server and can be used to log on to multiple computers on the network.

[2] Local user accounts are those accounts that are stored locally on the individual computers and can only be used to log on to the computer in which the account is stored.

restricted. For example, the Town Clerk had access to payroll and employee information, including PPSI, that was not needed to carry out her job duties.

Further, the Town contracts with another vendor for assistance with bookkeeping duties. This individual shares the administrative aide’s account to perform his duties, making the audit trail ineffective because there is no way to differentiate between each user’s activities for this account. Further, the financial application’s data files were stored on a shared folder that all network users unnecessarily had full access to. This access allows users to create, open, view, modify and delete files; change permissions; and take ownership of existing files or perform transactions within the financial application and then remove evidence from the data files without detection.

These weak access controls existed because of a lack of communication between Town officials and the vendor. Users also shared their credentials for ease of use. Unnecessary accounts that are not disabled as soon as they are no longer needed increases the risk of unauthorized access and potential entry points for attackers to copy, manipulate or delete PPSI. Of particular risk are the accounts of non-employees, because their existence indicates a lack of timely account maintenance or monitoring. If these accounts were used by individuals for malicious activities, it may go undetected longer. Furthermore, accounts not assigned to specific individuals and shared credentials can prevent Town officials from tracing suspicious activity, presenting difficulties in holding the responsible user accountable for their actions. Consequently, the Town’s IT resources and data are at increased risk for loss or misuse.

The Board Lacked an IT Services Contract

The Town has contracted with its vendor for IT services for over 10 years and paid $16,269 during the audit period for related services. However, officials did not formalize the agreement identifying the specific services to be provided or the vendor’s responsibilities until June 2019. Except for identifying general services available to the Town including software support, network support, phone support, server/workstation maintenance, Wi-Fi support, firewall/router maintenance, data wiring and backup services, the contract does not include specific provisions. For example, the contract does not specifically identify the Town’s needs and expectations with the level of service to be provided by the vendor.

The Town also did not have a written SLA with its vendor to define service level objectives; performance indicators; roles and responsibilities; nonperformance impact; security and audit procedures; reporting requirements; review, update and approval processes; and payment and scope of services to be provided. The vendor communicated that the services listed are not exhaustive and additional services could be provided upon the Town’s request.

Without a formal contract and SLA, officials were not aware of the extent of services to be provided and could not ensure they were getting the services they were entitled to. Insufficient, nonexistent or vague agreements can contribute to confusion over who is responsible for various aspects of the IT environment, including data recovery in the event of a ransomware[3] attack or other security incident, which puts data and computer resources at greater risk for unauthorized access, misuse or loss.

Town Officials Did Not Adopt a Disaster Recovery Plan or Backup Procedures

Town officials have not developed, adopted and implemented a disaster recovery plan or formal backup procedures. Although computers connected to the network are backed up to the cloud[4] by the vendor on a daily basis, backups are not periodically tested. Additionally, there are no guidelines in place to delegate responsibilities or minimize effects to operations in the event of a disaster. Without a disaster recovery plan and formal backup procedures, the Town could lose important financial and other data. All responsible parties may not be aware where they should go, or how they will continue to do their jobs, to resume business after a disruptive event.

What Do We Recommend?

Town officials should:

1. Develop, adopt and implement policies and procedures for safeguarding IT resources.

2. Provide IT security awareness training to personnel who use IT resources.

3. Design and implement procedures to evaluate all existing network, local and administrator user accounts and disable any deemed unnecessary, including those with administrative access. Accounts should be periodically reviewed to determine whether they are appropriate and necessary.

4. Design and implement procedures to ensure unnecessary user permissions are removed and user accounts are not inappropriately shared.

[3] Ransomware is a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

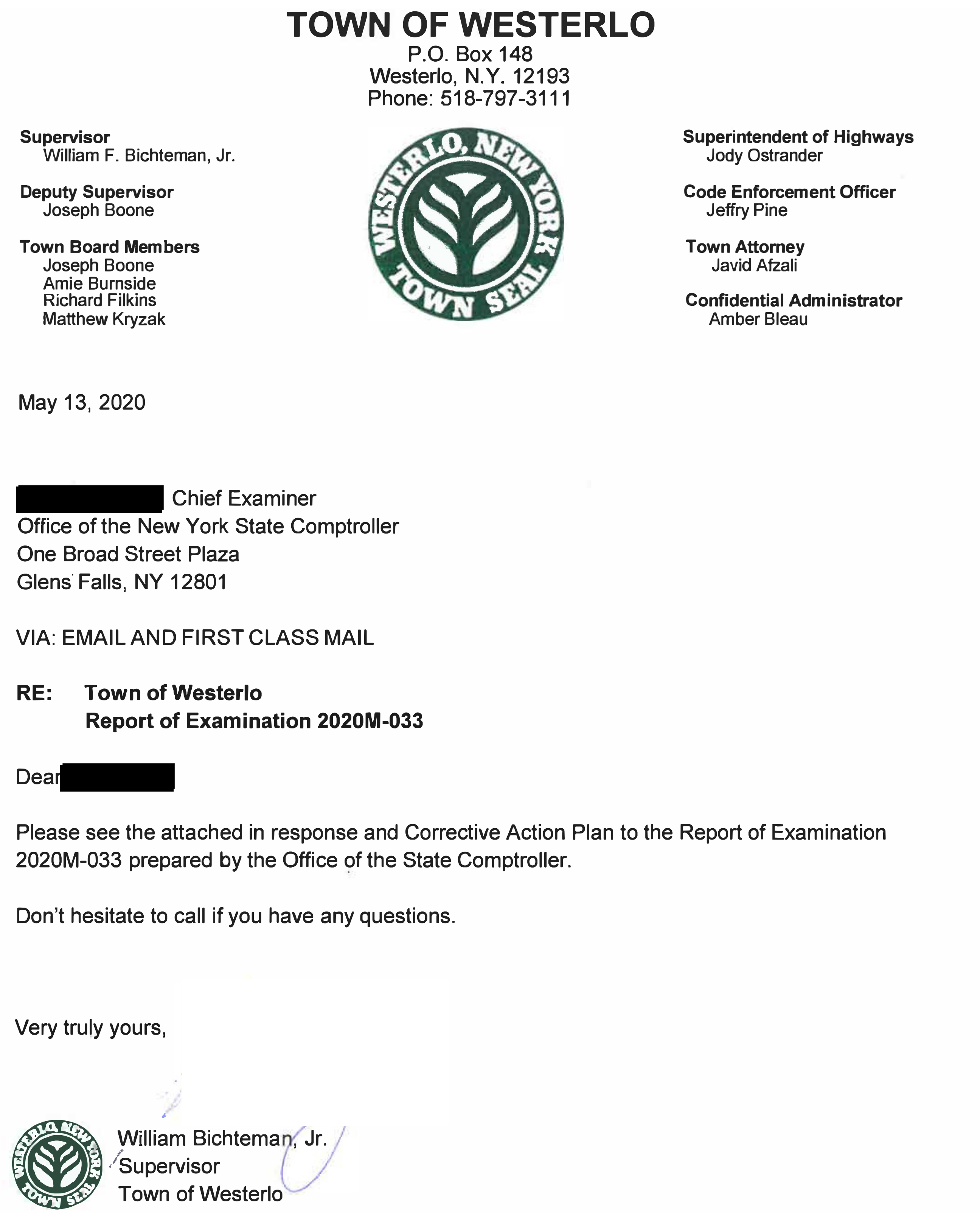
[4] Cloud-based storage makes it possible to save files to a remote storage location and retrieve them on demand.

5. Develop an SLA with the Town’s vendor to address the Town’s specific needs and expectations for IT services and ensure the vendor provides the agreed upon services.

6. Develop, adopt and implement a comprehensive disaster recovery plan and formal backup procedures.

Appendix A: Response From Town Officials

The Town officials' response has been included in its entirety except for sensitive information technology details that were redacted for security reasons.



TOWN OF WESTERLO

P.O. Box 148
Westerlo, N.Y. 12193
Phone: 518-797-3111

Supervisor
William F. Bichteman, Jr.

Deputy Supervisor
Joseph Boone

Town Board Members
Joseph Boone
Amie Burnside
Richard Filkins
Matthew Kryzak

Superintendent of Highways
Jody Ostrander

Code Enforcement Officer
Jeffry Pine

Town Attorney
Javid Afzali

Confidential Administrator
Amber Bleau

May 13, 2020

[redacted] Chief Examiner
Office of the New York State Comptroller
One Broad Street Plaza
Glens Falls, NY 12801

VIA: EMAIL AND FIRST CLASS MAIL

RE: Town of Westerlo
Report of Examination 2020M-033

Dear [redacted]

Please see the attached in response and Corrective Action Plan to the Report of Examination 2020M-033 prepared by the Office of the State Comptroller.

Don't hesitate to call if you have any questions.

Very truly yours,

William Bichteman, Jr.
Supervisor
Town of Westerlo

TOWN OF WESTERLO

P.O. Box 148
Westerlo, N.Y. 12193
Phone: 518-797-3111

Supervisor
William F. Bichteman, Jr.

Deputy Supervisor
Joseph Boone

Town Board Members
Joseph Boone
Amie Burnside
Richard Filkins
Matthew Kryzak

Superintendent of Highways
Jody Ostrander

Code Enforcement Officer
Jeffry Pine

Town Attorney
Javid Afzali

Confidential Administrator
Amber Bleau

May 13, 2020

[redacted] Chief Examiner
Office of the New York State Comptroller
One Broad Street Plaza
Glens Falls, NY 12801

VIA: EMAIL AND FIRST CLASS MAIL

RE: Town of Westerlo
Report of Examination 2020M-033

Dear [redacted]

In response to the Report of Examination 2020M-033 prepared by the Office of the State Comptroller, please accept this letter as the Town of Westerlo's response as well as our Corrective Action Plan (CAP). To organize the Town's replies, I have arranged our responses and Corrective Action Plans to correspond to the same order as the report.

Town Officials Have Not Developed and Communicated Adequate IT Policies

FINDINGS: *The Board has not adopted or implemented IT policies and procedures addressing acceptable computer use, access to PPSI, password security, or information security management. Without policies and procedures, Town officials and employees may not be properly aware of how to safeguard IT resources. In addition, the Board did not provide users with security awareness training to help ensure they understood security measures needed to protect the network because the Board lacked sufficient knowledge and experience related to IT.*

RESPONSE AND REMEDIAL ACTION: The Town does not dispute the finding.

As part of the overall Corrective Action Plan (CAP), the Town developed and adopted by Board Resolution a Town wide IT Policy February 18th, 2020. In addition, changes have been made to the Town's Employee Handbook to apprise employees of the Information Technology Policy and how it applies to them specifically.

Town Officials Did Not Implement Strong Access Controls

FINDINGS: *Town officials have not implemented comprehensive procedures for managing, limiting, securing, and monitoring user accounts. Town officials relied on a vendor for account maintenance but did not have a process in place to ensure strong access controls were implemented. Specifically, officials did not adequately communicate their needs with the vendor. As a result, access rights and permissions for network, local, and financial application users were not properly granted based on job duties.*

RESPONSE AND REMEDIAL ACTION: The Town does not dispute the finding.

However, the Corrective Action Plan (CAP) to rectify the short comings is complex and must address many individual issues. The Town's Action Plan to address these particular findings is listed in five parts as follows:

[redacted]

[redacted]

The Board Lacked an IT Services Contract

FINDINGS: *The Town has contracted with its vendor for IT services for over 10 years and paid $16,269 during the audit period for related services. However, officials did not formalize the agreement identifying the specific services to be provided or the vendor's responsibilities until June 2019. Except for identifying general services available to the Town including software support, network support, phone support, server/workstation maintenance, Wi-Fi support, firewall/router maintenance, data wiring, and backup services, the contract does not include specific provisions. For example, the contract does not specifically identify the Town's needs and expectations with the level of service to be provided by the vendor.*

The Town also did not have a written SLA with its vendor to define service level objectives; performance indicators; roles and responsibilities; nonperformance impact; security and audit procedures; reporting requirements; review, update and approval process; and payment and *scope of services to be provided. The vendor communicated that the services listed are not exhaustive and additional services could be provided upon the Town's request.*

RESPONSE AND REMEDIAL ACTION: The Town does not dispute the finding.

As an integral part of our CAP, the Town recognizes that a written Service Level Agreement (SLA) is necessary and provides the foundation for the Remedial Actions proposed. The Town has and will continue to solicit the services of IT support companies to institute the Town's IT Policy as well as the Towns specific needs and expectations. The IT Policy recently adopted will be revised to ensure the SLA includes [redacted] Backup Procedure, and incorporated Disaster Plan adopted by the Town Board.

Town Officials Did Not Adopt a Disaster Recovery Plan or Backup Procedures

FINDINGS: *Town officials have not developed, adopted, and implemented a disaster recovery plan or formal backup procedures. Although computers connected to the network and are backed up to the cloud by the vendor on a daily basis, backups are not periodically tested. Additionally, there are no guidelines in place to delegate responsibilities or minimize effects to operations in the event of a disaster.*

RESPONSE AND REMEDIAL ACTION: The Town does not dispute the finding and identifies the need for backup procedures and a recovery plan.

The server and connected computers are backed up daily. The system power has battery backup supporting standby generator auto start. The Towns current IP provider will be retained to help develop the Disaster Recovery/Backup Plan. The SLA will include provisions allowing the Supervisors Office to monitor and verify daily data and operating system backups.

Summation

The Town officials recognize the importance of protecting, maintaining, and safeguarding the valuable IT resources in trusted to them.

The review and audit conducted by the Office of the State Comptroller (OSC) has been both helpful and enlightening. Since March of 2019, the Town Board has been steadily working to improve the IT security controls. Simultaneously we have expanded our computer network to enable the Town offices to function at a higher level and in harmony with our Federal, State, and County agencies.
As reported, many of the specific vulnerabilities highlighted within the report have been addressed or are being reviewed.

Ideally, the Town would like to enact the elements of our Corrective Action Plan (CAP) immediately. However, the time frame for development and enactment are dependent on several factors. First is the matter of soliciting IT providers, second is appropriation of the funding to eliminate the weakness identified in the audit and report, and finally the negative effect COVID-19.

Soliciting IT providers and evaluation of an SLA warrants due diligence to ensure the agreement is comprehensive and addresses all the controls necessary to our specific environment. The major issues i.e.; Access Control, [redacted] and Backups can be rectified relatively quickly by working with the Town's current IT firm without having a new SLA in place and it is the goal of the Town to precede as quickly as possible.

The available funding is a significant factor. There are no funds available in the 2020 Town budget for an IT professional to undertake the scope of services necessary to meet the expectations of the OSC Audit and Report. To complicate further, we must anticipate revenue losses as a result of the COVID-19 virus. At this time, the Town has little choice but to propose the expenditure in the 2021 year.

The impact of COVID-19 on the entire process is overwhelming. The current virus outbreak has restricted the Town Board's ability to meet frequently and productively. It has become a major impediment to moving forward on not only this issue, but other serious issues as well. Accordingly, the deliberation process involving Board action has slowed down and approvals may take many months.

I wish to acknowledge the professional and courteous manner in which our audit was conducted. Myself and the other department heads appreciate the spirit of cooperation and patients displayed.

Finally, if you have questions regarding the foregoing, require further information, or would like to discuss the same please do not hesitate to contact me. I am hopeful that the Office of the State Comptroller recognizes that the Town of Westerlo is working diligently attempting to correct the deficiencies noted by OSC and will monitor our progress to ensure compliance with the standards set forth.

Very truly yours,

William Bichteman, Jr.
Supervisor
Town of Westerlo

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 Town officials, employees and the vendor to obtain an understanding of the Town's IT environment, internal controls and applicable processes, procedures and applications and determine whether there were any computer policies and whether Town personnel received cybersecurity awareness training.
- We reviewed the written agreement between the Town and vendor for services provided.
- We analyzed and assessed all 12 network user accounts and 11 local user accounts on four computers and the server using specialized audit software. We selected the four computers and the server because they provided access to the Town's financial application.
- We compared results of our analyses to the Town's master employee list to determine whether any users who were no longer employed by the Town still had active user accounts enabled on the Town's network.

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 Town 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.

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 Town 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

GLENS FALLS REGIONAL OFFICE – Gary G. Gifford, Chief Examiner

One Broad Street Plaza • Glens Falls, New York 12801-4396

Tel (518) 793-0057 • Fax (518) 793-5797 • Email: Muni-GlensFalls@osc.ny.gov

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

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