OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT
& SCHOOL ACCOUNTABILITY

Village of Ilion

Information Technology

Report of Examination

Period Covered:

January 1, 2014 — October 31, 2014

2015M-34

Thomas P. DiNapoli

Table of Contents

State of New York
Office of the State Comptroller

Division of Local Government
and School Accountability

July 2015

Dear Village Officials:

A top priority of the Office of the State Comptroller is to help local government officials manage government resources efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support government operations. The Comptroller oversees the fiscal affairs of local governments statewide, as well as compliance with relevant statutes and observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations and Village Board governance. Audits also can identify strategies to reduce costs and to strengthen controls intended to safeguard local government assets.

Following is a report of our audit of the Village of Ilion, entitled Information Technology. This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law.

This audit's results and recommendations are resources for local government officials to use in effectively managing operations and in meeting the expectations of their constituents. If you have questions about this report, please feel free to contact the local regional office for your county, as listed at the end of this report.

Respectfully submitted,

Office of the State Comptroller
Division of Local Government
and School Accountability

State of New York
Office of the State Comptroller

EXECUTIVE SUMMARY

The Village of Ilion (Ilion) is located in the Towns of German Flatts and Frankfort, in Herkimer County, and has a population of approximately 8,000. The Village is governed by an elected Board of Trustees (Board) responsible for the general oversight of Village operations and the design and implementation of internal controls to safeguard Village assets. The Village contracted with an information technology (IT) consultant who administers its network and with a software vendor who serves as the administrator of the Village's financial software.

The Village provides residents with various services including water, electric, public safety, street maintenance and general government support. The Water Treatment Supervisor is responsible for the Village's water treatment operations. The Village's Water Department (Water Department) maintains a computer-based system. The Village contracted with two water system vendors who, along with Water Department personnel, maintain the Village's water system.

The Village's budgeted appropriations for the 2014-15 fiscal year total $13.6 million, which includes approximately $6.4 million in the general fund and $1.4 million in the water fund.

Scope and Objective

The objective of our audit was to examine the IT controls over the Village's electronic data and computer resources and the Water Department's system for the period January 1 through October 31, 2014. Our audit addressed the following related questions:

- Did Village officials implement IT security controls to adequately safeguard electronic data and computer resources?

- Did Village officials implement IT controls to adequately safeguard electronic access to the Water Department's system?

Audit Results

We found deficiencies in the IT controls over the Village's electronic data and computer resources that left these assets vulnerable to electronic threats. In 2014, the Village experienced two IT security incidents initiated by falsified email messages with a malware attachment that, when opened by employees, converted stored Village data into encrypted (unreadable) format. This "ransomware" directed the users to make ransom payments to allow decryption of the data.[1] Village employees had

[1] The Village ultimately made the ransom payments, totaling $800.

not been trained in recognizing and properly responding to such falsified email, and the Village's disaster recovery plan did not provide for sufficiently frequent backup of critical data nor include steps to take upon detection or occurrence of IT security incidents. Additionally, the Village did not have a breach notification policy or local law requiring notification of affected parties when there is a security breach relating to private information. Because officials did not take steps to determine the extent of the incidents, they could not be certain whether one or both incidents constituted a breach that would have required notification to affected individuals. Although additional antivirus software was installed and training provided after the two incidents, these measures were not timely or thorough enough to significantly reduce the risk of such incidents recurring.

We also found that, in the absence of an acceptable-use policy, Village employees used the Internet to access websites of a non-business or personal nature, placing Village IT assets at an increased risk from malware commonly spread through such sites. Further, Village officials have not established procedures to manage user access to the Village's financial program. Of 22 user accounts, six were created for users who are no longer Village employees; four were generic accounts used by more than one person, therefore removing individual accountability for any inappropriate actions; and one user account included permissions not required by the employee's job duties, allowing potential misuse such as the creation of new user accounts or changes to user passwords. The use of obsolete and generic user accounts and unnecessary permissions increases the risk of unauthorized or inappropriate use of the Village's IT assets.

In addition, the written agreement between the Village and its IT consultant for support services did not explicitly define the consultant's activities, leading to an inconsistent understanding of responsibilities, which could allow gaps in IT security.

Finally, the Village has not established a process for staying current on water system cybersecurity threats. Village officials do not receive alerts to such threats from either the U.S. Department of Homeland Security's Industrial Control System Cyber Emergency Response Team (ICS-CERT) or the Water Information Sharing and Analysis Center (WaterISAC). One of the alerts issued by ICS-CERT warns of threats related to Internet-facing (directly connected to the Internet) control systems devices. Attackers can use automated tools to easily identify exposed controls systems, posing an increased risk of attack. Despite these risks, neither the Water Department personnel nor water system vendors monitor for Internet-facing Village water system devices.

Comments of Local Officials

The results of our audit and recommendations have been discussed with Village officials, and their comments, which appear in Appendix A, have been considered in preparing this report. Village officials generally agreed with our recommendations and indicated they planned to initiate corrective action.

Introduction

Background

The Village of Ilion (Ilion) is located in the Towns of German Flatts and Frankfort, in Herkimer County, and has a population of approximately 8,000. The Village is governed by an elected Board of Trustees (Board) which comprises the Mayor and four Trustees. The Board is responsible for the general oversight of Village operations and the design and implementation of internal controls to safeguard Village assets.

The Village provides residents with various services including water, electric, public safety, street maintenance and general government support. The Village uses a variety of electronic data and computer resources to provide these services. The Village contracted with an information technology (IT) consultant who administers the network, configures and repairs computer systems and diagnoses system or network issues. The Village also contracted with a software vendor who serves as the administrator of the Village's financial software.

The Village provides water services to over 9,000 residential and commercial customers inside and outside the Village. The Village's Water Department (Water Department) maintains a computer-based system to monitor water flows, levels, pressure and quality. The Water Treatment Supervisor is responsible for the Village's water treatment operations. The Village contracted with two water system vendors who designed, engineered, implemented and, along with the Water Department personnel, maintain the Village's water system.

The Village's budgeted appropriations for the 2014-15 fiscal year total $13.6 million, which includes approximately $6.4 million in the general fund and $1.4 million in the water fund.

Objective

The objective of our audit was to examine IT controls over the Village's electronic data and computer resources and the Water Department's system. Our audit addressed the following related questions:

- Did Village officials implement IT security controls to adequately safeguard electronic data and computer resources?
- Did Village officials implement IT controls to adequately safeguard electronic access to the Water Department's system?

Scope and Methodology

We examined the Village's IT controls for the period January 1 through October 31, 2014. Because of the sensitivity of some of this information, we did not discuss certain audit results in this report, but instead communicated them confidentially to Village officials.

We conducted our audit in accordance with generally accepted government auditing standards (GAGAS). More information on such standards and the methodology used in performing this audit is included in Appendix B of this report.

Comments of Local Officials and Corrective Action

The results of our audit and recommendations have been discussed with Village officials, and their comments, which appear in Appendix A, have been considered in preparing this report. Village officials generally agreed with our recommendations and indicated they planned to initiate corrective action.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and forwarded to our office within 90 days, pursuant to Section 35 of the 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 this plan available for public review in the Village Clerk's office.

Electronic Data and Computer Resources

The Village uses a variety of electronic data and computer resources to provide services to residents. These valuable assets must be secured against unauthorized access, misuse and abuse. This is especially important given the increase in system attacks including viruses, worms and other types of malware.[2] We found deficiencies in the IT controls over the Village's electronic data and computer resources, including inadequate preparation for responding to IT security incidents, unnecessary user accounts, excessive user permissions to financial software and inconsistent understanding of IT security responsibilities. As a result, Village IT assets are at risk of attacks that could lead to unauthorized access to or disclosure of sensitive information, inappropriate modification or deletion of critical data or interruption of service availability. In fact, the Village experienced two IT security incidents in 2014.

Ransomware Incidents

Ransomware is a type of malware that restricts access to a computer (or computer system) that it infects and demands that a ransom be paid in order for the computer user to regain access to their computer or the electronic data contained on it. IT best practices suggest that ransomware victims consult cybersecurity experts and law enforcement prior to making any ransom payments and review (or contract for the review of) audit logs and other available information to determine the extent of any incidents that occur. In addition, New York State Technology Law (State Technology Law) requires municipalities and other local agencies to have a breach notification policy or local law. Such policy or local law must require that

[2] Malware, short for malicious software, refers to software programs that are specifically designed to harm computer systems and electronic data. Malware often causes this harm by deleting files, gathering sensitive information and making systems inoperable. Computer users can inadvertently install malware on their computers in many ways, including opening email attachments, downloading free software from the Internet or merely visiting infected websites.

notification be given to certain individuals[3] when there is a breach of the security of the system as it relates to private information.[4]

Proper IT security and preparation can reduce the risk of becoming a victim of ransomware and data breaches. This includes providing IT security training to all employees, implementing and enforcing an acceptable-use policy, maintaining offline backup copies of all critical data, limiting the number of users granted administrative privileges,[5] installing and keeping antivirus protection up-to-date and applying software patches and updates in a timely manner.

The Village experienced two IT security incidents in 2014, both of which involved ransomware. The incidents were initiated by falsified email messages with malware attached. When Village employees opened the malicious attachments, all data accessible to the program (which included all data stored on and shared with the system because both employees had administrative privileges to their systems) was converted into an encrypted format, making that data unreadable and unusable until decrypted. As a result, all users were unable to process Village transactions on the system. The program then directed the employees to make a ransom payment to obtain the keys needed to decrypt the data. However, Village officials did not determine the extent of the incidents and therefore did not know whether a data breach had actually occurred. In both instances, the Mayor, IT consultant and appropriate Village employee discussed the circumstances and ultimately decided to make the ransom payments. These payments were made on January 10, 2014 in the amount of $300 and on May 9, 2014 in the amount of $500, the same days as

---

[3] New York State Technology Law generally provides that notification shall be given by written notice, electronic notice, telephone notification or substitute notice to any resident of New York State whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The law further requires that the disclosure be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement.

[4] State Technology Law generally defines "breach of the security of the system" as meaning unauthorized acquisition of computerized data which compromises the security, confidentiality or integrity of personal information maintained by the entity. "Private information" is defined as personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired: (1) social security number; (2) driver's license number or non-driver identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code or password which would permit access to an individual's financial account.

[5] Administrative privileges allow users to access all data on a system, including data created and stored by other users; make changes to the settings configured on the system, including disabling antivirus software; and create new user accounts or change the levels of privileges granted to existing user accounts.

the attacks. In both instances, Village officials purchased a prepaid disbursement card and the IT consultant entered the card numbers into the program to receive the decryption keys. While both the Board and local law enforcement were informed of the incidents, the payments were not presented to the Board for approval and formal reports with law enforcement were not filed.

Incident Preparation and Analysis – Village employees were inadequately prepared for responding to IT security incidents. At the time the incidents occurred, employees had not received training or other guidance on how to recognize and respond to falsified email messages. The Village's disaster recovery plan[6] did not include guidelines for ensuring that all critical data is backed up at a sufficient frequency, steps that should be taken upon detection of an IT incident or procedures for analyzing audit logs[7] or other forensic data after an IT incident occurs. While Village officials notified local law enforcement of the incidents, they did not file formal reports and did not have any analysis done of the affected computers. As a result, Village officials did not determine the extent of the incidents. In addition, the Village did not have a breach notification policy or local law in place as required. Since Village officials did not take steps to determine the extent of the incidents, they cannot be certain whether one or both of the incidents constituted a breach that would have required notification to affected individuals. Village officials also did not consider or discuss potential consequences of the incidents, such as sensitive data exposure or residual system infection.[8] We performed a limited analysis and identified evidence that indicates that one or more Village systems may currently be infected with malware or compromised in some other manner. We provided the results of our analysis to Village officials for follow-up.

Post-Incident Activity – The Board has not established a policy or other written guidance related to incident response since the two incidents occurred. As a result of the incidents and to help prevent recurrences, the Village's IT consultant indicated that he installed more sophisticated antivirus software on the Village's systems and provided IT security awareness training to some Village employees. However, the antivirus software was installed approximately seven months after the first incident and three months after the second incident, and the training was provided nearly eight and four months after the first and second incidents, respectively. This training was

[6] A disaster recovery plan is a documented process to be followed in response to a disaster or other significant incident.

[7] Automated trails of user activity on the system

[8] Malware often includes programs that remain hidden on infected systems after more obvious signs of infection are removed. Attackers use these residual programs to access the data on systems days, weeks, months and even years after the initial infection.

not mandatory. These actions alone have not significantly improved the Village's IT security posture or minimized the risk that this type of IT security incident could recur.

Rather, we found that Village employees engage in activities that continue to put the Village at risk. Specifically, we identified evidence of questionable Internet use on six of the eight Village workstations that were not connected to the Village's internal network. Village employees used these workstations to access multiple websites of a personal, non-business or otherwise high-risk nature, including social networking, dating, auction and job search websites. Because these types of websites are commonly used to spread malware, such Internet use unnecessarily exposes the Village's workstations and data to future IT security incidents. The Board has not adopted an acceptable-use policy that would help Village employees understand their responsibilities and expected behavior with regard to using Village IT assets.

User Access

The Village uses a software program to manage financial records and related personal, private and sensitive information. It is essential that Village officials protect this valuable resource from unauthorized or inappropriate use. To minimize the risk of such use, IT security best practices limit user access to that necessary for officials and employees to perform their job duties. However, we found that Village officials have not established procedures for managing user access to this program. User accounts are not required to be authorized by a department manager prior to creation and user permissions are not monitored to ensure they are modified and removed as needed. We evaluated the program access granted to users and found unnecessary user accounts and excessive user permissions. Of all 22 user accounts in the program:

- Six user accounts were created for individuals no longer employed by the Village. Failing to remove or disable accounts that were created for former employees puts the Village at risk that a disgruntled individual could use the account to inappropriately access, modify, delete or otherwise corrupt Village data.

- Four user accounts were generic accounts used by more than one individual. The use of generic accounts can prevent the Village from tracing suspicious activity to a specific individual and holding that person accountable for inappropriate actions.

- One user account was granted permissions not necessitated by the employee's job duties. According to the software vendor,

these permissions could be abused or inadvertently used to create new user accounts or change other users' passwords.

By allowing the use of obsolete and generic user accounts and unnecessary permissions, Village officials are increasing the risk of unauthorized or inappropriate use of, and potential damage to, the Village's IT assets.

IT Services Contract

The Village contracted with a consultant for IT support services. According to the written agreement, the consultant is responsible for "the repair, service or replacement of all information technology hardware and associated equipment," excluding issues outside normal equipment usage. The agreement does not explicitly define the activities to be performed in fulfilling these responsibilities. Further, while the agreement allows the consultant to provide other services for an additional fee, the invoices submitted to the Village show that the consultant has performed multiple services outside the scope of the agreement, including those related to IT security, without charging additional fees. Village officials could interpret this to mean that those activities are part of the scope of the agreement and that they can and should expect the consultant to continue such activities in the future. These deficiencies in contracting practices have contributed to confusion over responsibilities for IT security at the Village. For example, the Village Treasurer indicated that the consultant is responsible for sanitizing hardware prior to disposal, while the consultant contended that hardware sanitization is not his responsibility.

Inconsistent understanding of responsibilities often allows gaps in IT security practices. The failure to perform essential IT security tasks, such as applying security patches and managing user permissions, could leave Village systems and data vulnerable to attack. Successful attacks could lead to unauthorized access to or disclosure of sensitive information, inappropriate modification or deletion of critical data or interruption of service availability.

Recommendations

The Board should:

1. Provide IT security awareness training to all Village employees. This training should cover how to recognize and respond to falsified email messages and the risks of inappropriate Internet use.

2. Amend the Village's disaster recovery plan to incorporate information that would aid Village officials in effectively and efficiently responding to and recovering from future IT security incidents, including ransomware infections.

Amendments to consider include the definition and examples of an IT security incident, the definition and locations of critical data, procedures for backing up and restoring data and the steps that should be taken after an incident occurs.

3. Periodically test the disaster recovery plan to help ensure that employees are aware of their assigned duties in the event an incident occurs and that backup and restoration functions properly for all critical data.

4. Establish and implement procedures to ensure audit logs are periodically reviewed, in a timely manner, for suspicious activity.

5. Adopt a breach notification policy or local law consistent with the requirements of State Technology Law.

6. Review the information provided to the Village related to our analysis and take corrective actions as necessary to remediate any Village systems that may have been compromised.

7. Adopt an acceptable-use policy that defines acceptable and unacceptable activities when using Village workstations, networks and other IT assets.

8. Review the user access granted to the Village's financial software and take corrective actions as necessary.

9. Review the terms of current and future contracts for IT support services to ensure they explicitly define and accurately reflect the activities the Village expects the vendor to perform.

Water Department System

The Village's Water Department maintains a computer-based system to monitor water flows, levels, pressure and quality characteristics (such as pH, turbidity and chlorine residual). A disruption to this system could range from a minor inconvenience to serious consequences relating to the health of both employees and water consumers.

Despite this risk, the Village has not established a process for staying current on water system cybersecurity threats. Village officials do not receive alerts to such threats from either the U.S. Department of Homeland Security's Industrial Control System Cyber Emergency Response Team (ICS-CERT) or the Water Information Sharing and Analysis Center (WaterISAC).

One of the alerts issued by ICS-CERT warns of threats related to Internet-accessible devices. This alert states that search engines may be proactively used by water system owners, operators and security personnel to locate Internet-facing devices (directly connected to the Internet) that may be susceptible to compromise. ICS-CERT encourages control system owners and operators to query various search engines to determine if their water system devices are found within the search results. If system devices are found using these tools, personnel responsible for Village IT assets should take the necessary steps to remove these devices from direct or unsecured Internet access as soon as possible.

Attackers may be able to leverage any Internet-accessible Village water system device to attack the Village's water system via the Internet. Such attacks could attempt to inappropriately modify water data, causing operators to take actions based on inaccurate information. This could ultimately lead to water shortage, loss, flooding or contamination. We found that neither the Village's Water personnel nor water system vendors monitor for Internet-facing Village water system devices. We performed a search engine query as encouraged by ICS-CERT and provided the results to Village officials. The Water Treatment Supervisor indicated he has begun coordinating with the Village's water system vendors to ensure the water system is as isolated from the Internet as possible.

Recommendations

The Board should establish and implement processes for:

10. Receiving and assessing security alerts from professional organizations such as ICS-CERT and WaterISAC.[9]

[9] This professional organization provides key information for water personnel to protect their systems from cybersecurity threats.

11. Regularly monitoring for Internet-facing Village water system devices that may be susceptible to compromise.

APPENDIX A

RESPONSE FROM LOCAL OFFICIALS

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

Village of Ilion
49 Morgan Street
Ilion, NY 13357
Phone: 315-895-7449
TDD 711

April 17, 2015

Office of State Comptroller
Ms. Rebecca Wilcox, Chief Examiner
State Office Bldg., Room 409
333 E. Washington St.
Syracuse, NY 13202-1428

Dear Chief Examiner:

At a special meeting held on April 15, 2015 the Board of Trustees of the Village of Ilion, NY reviewed the Draft Information Technology Report of Examination (2015M-34); along with all of its recommendations. The Board of Trustees agreed with the recommendations cited and will adopt and implement a comprehensive Information Technology Policy which addresses those recommendations.

A written Corrective Action Plan (CAP) will be submitted to your offices within 90 days of the filing of the final report.

Gratefully,

Mr. Terry A. Leonard
Mayor, Village of Ilion,

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

The objective of our audit was to examine the IT controls over the Village's electronic data and computer resources and the Water Department's system. To achieve our audit objectives and obtain valid evidence, we performed the following procedures:

- We interviewed Village officials, Water Department personnel and relevant third parties to obtain an understanding of the Village's network and water system environments and related IT controls.

- We inquired about any IT security incidents that have occurred at the Village and reviewed relevant documentation.

- We analyzed the audit logs generated by the Village's firewall for characteristics common to malware infections.

- We examined Internet use on the eight workstations not connected to the Village's internal network.

- We evaluated the user accounts and permissions granted to the Village's financial software.

- We reviewed the Village's procurement policy and the written agreement between the Village and the consultant providing IT support services. We then examined the invoices submitted by the consultant to the Village and interviewed the Village Treasurer and consultant regarding these services.

- We reviewed relevant water system reports, including the Village's Emergency Response Plan and Vulnerability Assessment, the Department of Health's inspection report and relevant water flow reports.

- We performed a query using the SHODAN search engine for the relevant Village public Internet Protocol (IP) address.

We conducted this performance audit in accordance with GAGAS. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

APPENDIX C

HOW TO OBTAIN ADDITIONAL COPIES OF THE REPORT

To obtain copies of this report, write or visit our web page:

Office of the State Comptroller
Public Information Office
110 State Street, 15th Floor
Albany, New York 12236
(518) 474-4015
http://www.osc.state.ny.us/localgov/

APPENDIX D

OFFICE OF THE STATE COMPTROLLER
DIVISION OF LOCAL GOVERNMENT
AND SCHOOL ACCOUNTABILITY

Andrew A. SanFilippo, Executive Deputy Comptroller
Gabriel F. Deyo, Deputy Comptroller
Nathaalie N. Carey, Assistant Comptroller

LOCAL REGIONAL OFFICE LISTING

BINGHAMTON REGIONAL OFFICE
H. Todd Eames, Chief Examiner
Office of the State Comptroller
State Office Building - Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313
Email: Muni-Binghamton@osc.state.ny.us

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

BUFFALO REGIONAL OFFICE
Jeffrey D. Mazula, Chief Examiner
Office of the State Comptroller
295 Main Street, Suite 1032
Buffalo, New York 14203-2510
(716) 847-3647 Fax (716) 847-3643
Email: Muni-Buffalo@osc.state.ny.us

Serving: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming Counties

GLENS FALLS REGIONAL OFFICE
Jeffrey P. Leonard, Chief Examiner
Office of the State Comptroller
One Broad Street Plaza
Glens Falls, New York 12801-4396
(518) 793-0057 Fax (518) 793-5797
Email: Muni-GlensFalls@osc.state.ny.us

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

HAUPPAUGE REGIONAL OFFICE
Ira McCracken, Chief Examiner
Office of the State Comptroller
NYS Office Building, Room 3A10
250 Veterans Memorial Highway
Hauppauge, New York 11788-5533
(631) 952-6534 Fax (631) 952-6530
Email: Muni-Hauppauge@osc.state.ny.us

Serving: Nassau and Suffolk Counties

NEWBURGH REGIONAL OFFICE
Tenneh Blamah, Chief Examiner
Office of the State Comptroller
33 Airport Center Drive, Suite 103
New Windsor, New York 12553-4725
(845) 567-0858 Fax (845) 567-0080
Email: Muni-Newburgh@osc.state.ny.us

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester Counties

ROCHESTER REGIONAL OFFICE
Edward V. Grant, Jr., Chief Examiner
Office of the State Comptroller
The Powers Building
16 West Main Street – Suite 522
Rochester, New York 14614-1608
(585) 454-2460 Fax (585) 454-3545
Email: Muni-Rochester@osc.state.ny.us

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

SYRACUSE REGIONAL OFFICE
Rebecca Wilcox, Chief Examiner
Office of the State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, New York 13202-1428
(315) 428-4192 Fax (315) 426-2119
Email: Muni-Syracuse@osc.state.ny.us

Serving: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence Counties

STATEWIDE AUDITS
Ann C. Singer, Chief Examiner
State Office Building - Suite 1702
44 Hawley Street
Binghamton, New York 13901-4417
(607) 721-8306 Fax (607) 721-8313