OFFICE OF THE NEW YORK STATE COMPTROLLER

DIVISION OF LOCAL GOVERNMENT
& SCHOOL ACCOUNTABILITY

Onteora Central School District

Information Technology

Report of Examination

Period Covered:

July 1, 2013 — November 5, 2014

2015M-92

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 School District Officials:

A top priority of the Office of the State Comptroller is to help school district officials manage their districts efficiently and effectively and, by so doing, provide accountability for tax dollars spent to support district operations. The Comptroller oversees the fiscal affairs of districts statewide, as well as districts' 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 Board of Education governance. Audits also can identify strategies to reduce costs and to strengthen controls intended to safeguard district assets.

Following is a report of our audit of the Onteora Central School District, 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 district 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 Onteora Central School District (District), located in Ulster County, serves students in the Towns of Hurley, Marbletown, Olive, Shandaken and Woodstock. In addition, the District serves some parcels of the Town of Lexington located in Greene County. The District is governed by a Board of Education (Board), which comprises seven elected members. The Board is responsible for the general management and control of the District's financial and educational affairs.

The Superintendent of Schools is the District's chief executive officer and is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction. The District Treasurer is responsible for accounting for the District's finances, maintaining the accounting records and preparing financial reports. The District has two primary schools, one intermediate school and one middle-high school, with an enrollment of approximately 1,400 students.

The District contracts with the Ulster County Board of Cooperative Educational Services (BOCES) for two network support specialists to provide technical assistance and support for the District's network and other information technology (IT) functions. The District also pays the high school and intermediate school principals a stipend to oversee the software applications used for the student management system. Additionally, two teachers are paid a stipend to be the first level of support and contact for IT issues within the school buildings.

Scope and Objective

The objective of our audit was to determine whether the District's IT assets were adequately safeguarded for the period July 1, 2013 through November 5, 2014. We extended our review of data extracted from the District's computers and networks through the end of our fieldwork March 3, 2015. Our audit addressed the following related question:

- Did the Board and District officials provide adequate oversight of IT assets?

Audit Results

The Board and District officials need to improve controls over the District's IT assets. We found that the Board did not establish an adequate acceptable use policy, a computer security plan, a disaster recovery plan, policies and procedures for the disposal of computer equipment or a policy for security awareness training. In addition, the District's service level agreement (SLA) with the BOCES for network support specialists did not include written terms defining the service level objectives and performance indicators, roles and responsibilities, nonperformance impact, security procedures,

reporting requirements, and, review/update and approval processes. The SLA also did not clearly identify who was responsible for various aspects of the District's IT environment. Without these policies and a comprehensive SLA, the Board does not have adequate assurance that employees and contractors understand their responsibilities to ensure that the District's IT assets are secure.

We also found that the District did not keep an inventory of software licenses and its hardware inventory records were not accurate and up-to-date. Of the 31 items that should have been tagged and entered into the inventory system, 18 items (or 58 percent), including tablets and wireless streaming devices, were not included in the inventory system. Without an accurate inventory of computer and technology equipment, District officials cannot be assured that these assets are adequately accounted for and protected from loss, theft, misuse and obsolescence. Further, District officials cannot ensure that the software programs were authorized by IT management and licenses were obtained legally, as required by the District's acceptable use policy. Furthermore, although the District used a program to filter web content, we identified sites that were not reviewed for actual content. We reviewed 35 sites visited in the "unknown" category and found that 13 sites had content in blocked categories. As a result, users could access inappropriate websites and put the District's network at risk.

Comments of District Officials

The results of our audit and recommendations have been discussed with District officials, and their comments, which appear in Appendix A, have been considered in preparing this report. District officials generally agreed with our recommendations and plan to take corrective action.

Introduction

Background

The Onteora Central School District (District), located in Ulster County, serves students in the Towns of Hurley, Marbletown, Olive, Shandaken and Woodstock. In addition, the District serves some parcels of the Town of Lexington located in Greene County. The District is governed by a Board of Education (Board), which comprises seven elected members. The Board is responsible for the general management and control of the District's financial and educational affairs.

The Superintendent of Schools is the District's chief executive officer and is responsible, along with other administrative staff, for the District's day-to-day management under the Board's direction. The District Treasurer is responsible for accounting for the District's finances, maintaining the accounting records and preparing financial reports. The District has two primary schools, one intermediate school and one middle-high school, with an enrollment of approximately 1,400 students. During the 2013-14 fiscal year, the District had general fund expenditures of $56.3 million, which were funded primarily with real property taxes and State aid. The District's budgeted appropriations for the 2014-15 fiscal year were $51.9 million.

The District contracts with the Ulster County Board of Cooperative Educational Services (BOCES) for two network support specialists to provide technical assistance and support for the District's computer network and other information technology (IT) functions. The District also pays the high school and intermediate school principals a stipend to oversee the software applications used for the student management system. Additionally, two teachers are paid a stipend to be the first level of support and contact for IT issues within the school buildings.

Objective

The objective of our audit was to determine whether the District's IT assets were adequately safeguarded. Our audit addressed the following related question:

- Did the Board and District officials provide adequate oversight of IT assets?

Scope and Methodology

We examined the District's internal controls over IT systems for the period July 1, 2013 through November 5, 2014. We extended our review of data extracted from the District's computers and networks through the end of our fieldwork March 3, 2015. Our audit disclosed areas in need of improvement concerning the oversight of IT operations. Because of the sensitivity of some of this information,

certain vulnerabilities are not discussed in this report but have been communicated confidentially to District officials so they could take corrective action.

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 are included in Appendix B of this report.

Comments of District Officials and Corrective Action

The results of our audit and recommendations have been discussed with District officials, and their comments, which appear in Appendix A, have been considered in preparing this report. District officials generally agreed with our recommendations and plan to take corrective action.

The Board has the responsibility to initiate corrective action. Pursuant to Section 35 of the General Municipal Law, Section 2116-a (3)(c) of the New York State Education Law and Section 170.12 of the New York State Regulations of the Commissioner of Education, 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, with a copy forwarded to the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. The Board should make the CAP available for public review in the District Clerk's office.

Information Technology

District officials are responsible for designing internal controls over IT resources that include policies and procedures designed to protect software, hardware and data from loss or misuse due to errors, malicious intent or accidents. Organizations need to have an understanding of the software they own, how it is used and how best to track user rights to ensure licensing compliance. Additionally, District officials must ensure that the District's computer assets are physically secured and tracked by maintaining a comprehensive, accurate inventory record that is periodically reviewed and updated.

The Board and District officials need to improve controls over the District's IT assets. The Board did not establish adequate IT policies and procedures. District officials did not maintain software inventories and the hardware inventory records were not accurate and up-to-date. We also found that service level agreements (SLA) for IT consultants do not adequately identify who is responsible for various aspects of the District's IT environment. Furthermore, we identified sites in the web filter that were not reviewed for actual content. As a result, the Board does not have adequate assurance that the District's IT assets are secure.

Policies and Procedures

Policies and procedures over IT are part of the internal control structure and provide criteria and guidance for computer-related operations of a school district. Effective protection of computing resources and data include the adoption of an acceptable use policy that informs users about appropriate and safe use of District computers, a security plan which identifies potential risks and how to reduce system threats, a disaster recovery plan with guidance for minimizing loss and restoring operations should a disaster occur and an asset disposal policy for the proper and timely sanitization and disposal of IT assets. The Board should periodically review and update these policies as necessary to reflect changes in technology or the District's computing environment. Computer users need to be aware of security risks and be properly trained in practices that reduce the internal and external threats to the network.

Acceptable Use – Although the District has established an acceptable use policy, it has not been updated since July 2008. The policy does not address the use of the approximately 400 tablet computers that the District has loaned to middle and high school students and some building staff. Because the use of the tablets is not addressed in the acceptable use policy, there is no requirement in place to ensure that the tablets are used in an appropriate and secure manner, which could

potentially expose the District to malicious attacks or compromise systems and data.

Computer Security – The Board has not developed a written computer security plan. A lack of a formal security policy leaves the District vulnerable to the risks associated with individual use, including viruses, spyware and other forms of malware that could potentially be introduced through nonwork-related websites or programs. The District's IT assets are more susceptible to loss or misuse when users are not aware of security risks and practices necessary to reduce those risks. The Board was not aware that it should create a computer security plan.

Disaster Recovery – The Board has not adopted a comprehensive disaster recovery plan to address potential disasters. This occurred because District officials relied on the IT contractor and staff to implement their informal plan for disaster recovery. Consequently, in the event of a disaster, District personnel have no guidelines or plan to follow to help minimize or prevent the loss of equipment and data or to appropriately recover data. Without a comprehensive disaster recovery plan, the District could lose important financial data and suffer a serious interruption in District operations.

Disposal of Computer Equipment – The Board has not adopted procedures for sanitizing hard drives and other electronic media before disposing of them. Because the District has not provided guidance for the timely destruction of hard drives, the District has not disposed of hard drives since July 2009. If sensitive and confidential information is not fully removed, it may be recovered and inappropriately used or disclosed by unauthorized individuals with access to the discarded equipment and media.

Security Awareness Training – The Board has not adopted a policy to ensure that network users are provided with IT security training to ensure they understand the security measures designed to protect the District's network and their responsibilities for protecting the District's network. For example, the District's network support specialist informed us that, during our audit fieldwork, two users gave out their email passwords during an email phishing attack and spam was sent out from their accounts. The District's email accounts were inaccessible for a day. Although the issue was resolved, this could have been prevented if users were aware of IT security concerns through security awareness training. Creating security awareness through training also helps to ensure that everyone understands his or her individual responsibilities. By not providing such training, the District's IT assets are more vulnerable to loss and misuse because

network users are not aware of security risks and practices needed to reduce those risks.

Service Level Agreement

In order to protect the District and to avoid potential misunderstandings, there should be a written agreement between the District and the IT service provider that states the District's needs and expectations and specifies the level of service to be provided by the independent contractor/vendor. The components of the SLA should include identifying the parties to the contract, definitions of terminology, term/duration of agreement, scope/subject limitations, service level objectives and performance indicators, roles and responsibilities, nonperformance impact, security procedures, audit procedures, reporting requirements, review/update process, approvals, pricing, billing and terms of payment. Ideally, the agreement should be reviewed by knowledgeable IT staff and/or legal counsel and periodically reviewed, especially if the IT environment or needs change significantly. Such contracts should establish measureable performance targets so that there is a mutual understanding of the nature and required level of service to be provided.

The District has a written agreement with BOCES for the service of two network support specialists to provide technical assistance and support for the District's network and other IT functions. One network support specialist works full-time onsite and another works part-time onsite at the District. The agreement defines the payment, duration of services and biweekly onsite hours for the network support specialists. However, the agreement is not a comprehensive SLA because it does not have written terms defining the service level objectives and performance indicators, roles and responsibilities, nonperformance impact, security procedures, reporting requirements, and review/update and approval processes.

The District's lack of a comprehensive SLA with the IT consultants could contribute to a lack of individual accountability for various aspects of the District's IT environment. As a result, the District's data and computer resources are at greater risk for unauthorized access, misuse or abuse.

Hardware Inventory

Good business practices require management to maintain proper records of IT assets and perform a periodic physical inventory. Accurate and complete inventory lists help to ensure that assets are accounted for properly. A detailed inventory record should include a description of each item, including make, model and serial number; the name of the employee to whom the equipment is assigned, if applicable; the physical location of the asset; and relevant purchase information including acquisition date. Each item also should be affixed with identification tags for identification. Equipment should

be periodically examined to establish condition and to ensure none has been misplaced or stolen.

The District's IT hardware inventory records were incomplete and inaccurate. The District's stores clerk keeps an inventory list of all assets, including computers and computer-related equipment. We identified 107 purchases of computers and computer-related equipment made during our audit period. We randomly selected 31 items that should have been tagged and entered into the inventory system and traced them to the District's inventory records. Eighteen items (or 58 percent), including tablets and wireless streaming devices, were not included on the inventory system.

Without an accurate inventory of computer and technology equipment, District officials cannot be assured that these assets are adequately accounted for and protected from loss, theft, misuse and obsolescence. Further, in the event of a disaster, the District would be unable to provide the insurance company with an accurate list of assets and District officials would not know what they needed to replace.

Software Licenses

The purpose of a software license is to grant an end user permission to use one or more copies of the software program. When a software package is sold, it is generally accompanied by a license from the manufacturer that authorizes the purchaser to use a certain number of copies of the software. Organizations must obtain licenses commensurate with the number of copies in use. Implementing a complete and comprehensive software inventory list is crucial to safeguard IT assets from potential unlicensed software being installed on computers. As a best practice, the list should include all District-owned software installed on computers and the number of copies currently in use. Furthermore, the list should be used in regularly reviewing all computers owned by the District to ensure that all software programs installed are properly approved and licensed and that District staff is in compliance with the District's acceptable use policy.[1]

The District did not have complete, centralized and up-to-date inventory record of software programs installed on computers. The District also did not have a list of the approved software programs that should be on the computers. Furthermore, there was no regular review of the software installed on machines.

[1] The District developed an acceptable use policy to provide employees with guidelines for IT asset use and security. Specifically, the policy prohibits staff from downloading software. It also requires that new software be requested through the building principals and purchased through IT management.

As a result of these weaknesses, we reviewed District computers[2] to determine if the software installed was authorized and properly supported with a valid license or other documentation,[3] when required. We reviewed the software on 23 computers and found approximately 750 different software installations, of which 66 required licensing. District officials could not provide documentation to adequately support the licensing for three software programs.[4] Because District officials did not maintain a complete, comprehensive and centralized list of software installed on machines and perform regular reviews of District computers, District officials cannot ensure that the software programs were authorized by IT management and licenses were obtained legally as required by the District's acceptable use policy.

The full-time network support specialist informed us that he sometimes discovered random software when he was working on District computers or when a staff member called with an issue about the software. Prior to our audit testing, the network support specialist reimaged the computers to ensure that all computers had the appropriate software. The network support specialist no longer allows users to install software on their computers.

Web Filters

Due to the global nature of the Internet, school districts today find that it is a nearly indispensable resource for conducting legitimate business and educational activities. However, in recent years, even experienced users have been susceptible to significant threats from cyber criminals who exploit the vulnerabilities of systems and software to gain unauthorized access to sensitive data. For example, computers can be infected by malicious software[5] that, unknown to users, installs a keystroke logger that captures computer user identification

---

[2] See Appendix B: Audit Methodology and Standards for information about how the samples were chosen. To determine our population without a reliable hardware inventory, we identified the number of employees.

[3] If a license key is not on file, then other forms of proof of purchase (e.g, purchase orders, receipts or similar documentation) are acceptable as proof.

[4] Of the three unsupported software programs identified, the District provided us with the original packaging for two of the software programs. However, there was no documentation inside the packaging to show that the software programs were purchased by the District.

[5] Malicious software (malware) is designed to infiltrate a computer system by circumventing network defenses, avoiding detection and resisting efforts to disable it. Malware includes computer viruses, Trojan horses, spyware, worms, rootkits and other forms of invasive contaminating software. It can be introduced to a computer system through, for example, web browsers and email attachments. It may also be disguised as genuine software coming from an official Internet site. After installation, malware can thwart intrusion detection systems. Malware can be used to steal confidential or personal information like social security numbers, credit card numbers, computer user identification and passwords and bank account information. Malware can target individual users, organizations and networks.

and password information. Hackers can later use this information to access networks, databases and even bank accounts, resulting in high risk of loss. Internet browsing increases the likelihood that users will be exposed to some form of malicious software that may compromise data confidentiality.

The District has Internet content filters on its network servers to block access to certain objectionable websites. The District's filtering software offers 83 available filtering categories for blocking and the District blocks 34 of these categories. Some examples of the District's blocked categories include confirmed and unconfirmed spam[6] sources, games, pornography, dating, social networking, online gambling and proxy avoids and anonymizers.

The District's Internet content filtering software logs information relating to the domains visited. We reviewed a usage report of the top 500 sites visited for one day and found a proxy avoid as one of the top visited sites. Proxy avoids and anonymizers allow users to direct data through a third-party server to access blocked sites and applications anonymously. The site was not blocked because it was listed under the filtering category "unknown." We requested an additional report of the top 500 accessed sites in the "unknown" category and reviewed 35[7] sites from that list. In the sample of the top-visited 25 "unknown" sites in a 24-hour period, eight were sites that are in categories blocked by the District, 10 sites are allowed and seven were truly unknown. In another random sample of 10 sites, five were sites in blocked categories and five were allowable. Some examples of the truly-blocked categories that were listed as "unknown" include proxy avoids, games and malware.[8]

The District allowed "unknown" sites because many of them are legitimate for District purposes. However, by allowing all sites in the "unknown" category to be visited without review, users were able to bypass the District's controls over website content. As a result, users could access inappropriate websites and put the District's network at risk.

---

[6] Spam is irrelevant or inappropriate messages sent on the Internet to a large number of recipients.

[7] We narrowed the list of 500 down to exclude IP addresses and combine sites with the same domain to get a population of 133 sites. We then selected the top 25 sites visited and another 10 sites as a random sample of the remaining 108.

[8] Malware is software that is intended to damage or disable computers and computer systems.

Recommendations

The Board should:

1. Update the District's acceptable use policy to include tablet computers.

2. Adopt IT policies and procedures related to:

    - Computer security.

    - Disaster recovery.

    - Disposal of computer equipment.

3. Ensure all network users receive IT security training.

4. Establish a written agreement with BOCES that states the District's needs and expectations and specifies the level of service to be provided by the network support specialists.

5. Establish a comprehensive inventory policy that defines procedures for tagging all new purchases as they occur, relocating assets, updating the inventory list and performing periodic physical inventories. Someone separate from the recordkeeping process should perform the periodic physical inventories and investigate any differences.

6. Maintain a complete, comprehensive software inventory list of all software that the District owns.

7. Formalize a policy to perform reviews of the software on District computers and compare the results to the District's inventory list.

8. Ensure that all software licenses are accounted for by purchase orders, license agreements or other supporting documentation which shows the number of licenses for each software item or package purchased.

9. Ensure that District IT personnel monitor Internet usage in the "unknown" web filter category for inappropriate content.

APPENDIX A

RESPONSE FROM DISTRICT OFFICIALS

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

ONTEORA CENTRAL SCHOOL DISTRICT

PO Box 300
BOICEVILLE, NY 12412

Victoria McLaren
Assistant Superintendent for Business

Tel (845) 657-8499
Fax (845) 657-8742

July 7, 2015

Tenneh Blamah
Chief Examiner of Local Government and School Accountability
33 Airport Drive, Suite 103
New Windsor, NY 12553-4725

Dear Examiner Blamah,

Thank you for the time your examiners spent in our district reviewing our information technology controls. We have received the draft audit report and found both the draft report and the exit interview to be productive in reviewing the findings with our key staff members.

Upon receipt of our final report, we will work to develop a comprehensive action plan to address the issues you have identified. We have already begun to correct some of the items discussed in the exit interview.

The Onteora Central School District respects and appreciates the efforts of the Comptroller's Office and will strive for continuous improvement in the area of Information Technology.

Sincerely,

Barbara Schnell
Board President

Victoria McLaren
Interim Superintendent of Schools

APPENDIX B

AUDIT METHODOLOGY AND STANDARDS

The objective of our audit was to examine internal controls over the District's IT systems for the period July 1, 2013 through November 5, 2014. To accomplish the objective of this audit, we performed the following procedures:

- We interviewed District officials and the contracted full-time network support specialist to obtain an understanding of the District's IT operations.

- We reviewed District records for any IT-related policies and procedures.

- We obtained a list of staff in each of the school buildings categorized by class subject. From each list, we randomly selected two staff rooms in which to review the computers. In addition, we selected five District officials' computers for review. We used specialized audit software to obtain a list of all software installed on each machine. We reviewed the installations for licensing requirements. We examined license agreements and purchase orders to determine if the District authorized all software and whether the District maintained proper licensing for the software installed on each of the machines reviewed.

- We randomly selected 10 invoices from 107 IT-related invoices for review. We documented important identification information for each of the IT assets contained in each purchase, traced the IT assets to the District's inventory records and physically located the IT assets that were not in the inventory records.

- We obtained and reviewed reports from the District's Internet content filter summarizing usage. We further reviewed the usage summaries for the specific filter category of "unknown."

- We reviewed the District's agreement with BOCES for the services of their network support specialists.

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

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