DIVISION OF LOCAL GOVERNMENT AND SCHOOL ACCOUNTABILITY

REPORT OF EXAMINATION | 2021M-32

Westhill Central School District

Information Technology

JULY 2021

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

Contents

Report Highlights

Westhill Central School District

Audit Objective

Determine whether Westhill Central School District (District) officials implemented adequate information technology (IT) controls over the District Office's network to safeguard personal, private and sensitive information (PPSI).

Key Findings

District officials did not implement adequate IT controls over the District Office's network to safeguard PPSI. District officials did not:

- Monitor employee Internet use.
  - Eight of 10 employees' computers we reviewed were used for personal Internet activity.
- Properly manage network user accounts.
  - We examined all 31 enabled network user accounts on the District Office domain controller. Six unneeded network user accounts, seven shared user accounts and three user accounts were found with unneeded administrative permissions.
- Provide formalized IT security awareness training to staff.

Sensitive IT control weaknesses were communicated confidentially to District officials.

Key Recommendations

- Monitor employee Internet use.
- Ensure network user accounts are properly managed.
- Provide IT security awareness training.

District officials generally agreed with our audit findings and recommendations and indicated they would take corrective action.

Background

The District serves the Towns of Geddes and Onondaga in Onondaga County.

The District is governed by a five-member Board of Education (Board) that is responsible for the general management and control of the District's financial and educational affairs. The Superintendent of Schools (Superintendent) is the chief executive officer and is responsible, along with other administrative staff, for day-to-day management.

The Director of Educational Technology (Director) is responsible for managing the District's IT operations and reports to the Superintendent.

Quick Facts	
District Office Network Accounts	31
Employees	333
Student Enrollment	1,730

Audit Period

July 1, 2019 – September 24, 2020

Information Technology

The District relies on its IT assets for Internet access, email and maintaining financial and student information which contains PPSI. PPSI is any information to which unauthorized access, disclosure, modification, destruction or use – or disruption of access or use – could have or cause a severe impact on critical functions, employees, customers (students), third-parties or other individuals or entities.

The District contracts with the Central New York Regional Information Center (CNYRIC) for IT-related services, including Internet access and filtering, firewall/intrusion detection, data support services, financial and student information system support, and security awareness training support. The Director, along with two full-time network administrators and one computer aide, are responsible for overseeing general computer system operations.

How Does an Acceptable Use Policy (AUP) Protect IT Assets?

A school district should have a written AUP that defines the procedures for computer, Internet and email use. The AUP should describe appropriate and inappropriate use of IT resources, management's expectations concerning personal use of IT equipment and user privacy and consequences for violating the AUP. Monitoring compliance with the AUP involves regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity and investigating and reporting such activity.

Internet browsing increases the likelihood that users will be exposed to malware (e.g., viruses, worms, Trojan horses and spyware) that may compromise data confidentiality, integrity or availability. District officials can reduce the risks to PPSI and IT assets by routinely monitoring Internet use and by configuring web-filtering software to block access to unacceptable websites and limit access to websites that do not comply with the AUP.

The District's AUP, entitled Response Use Policy/Employee Technology Use Agreement, states that staff must use the District's technology equipment and the network "primarily for educational, and professional or career development activities." Additionally, the AUP establishes that any use of District IT assets "for the purpose of operating a private or personal business" is unacceptable, limiting employee access rights to the requirements of each user's job responsibility. Other inappropriate, unauthorized or illegal uses include, but are not limited to, installing unauthorized software and disrupting any District IT assets. Employees who violate the AUP may have their access rights revoked or be subject to discipline consistent with the District's collective bargaining agreements or applicable laws.

The AUP further provides that employees should not expect privacy when using the system, as any data created, stored or used can be subject to access upon legally-enforceable access requests. Employees are provided a copy of the AUP during the on-boarding process and are required to sign, indicating that their use of the computer system will conform to the AUP's requirements.

Some District Computers Were Used for Personal Activities

We initially selected 10 employees whose job duties required them to have administrative access rights to the District's network and user computers, or had access to PPSI or other confidential information, to review the Internet browsing history on their user computers. These 10 employees had 12 computers assigned to them. However, web history data from the Superintendent's computer was incompatible with our conversion and analysis tool. As a result, we could not determine whether he had personal Internet use. Therefore, we reduced our sample to 11 computers assigned to nine employees for our analysis of web history data.

Of the 11, one computer's website history was deleted around the time the user employee was notified of our audit test; therefore, we reviewed two days' of web history on this particular user computer. We identified eight employees who accessed websites not related to District operations, including the employee who deleted his history before our test. Two of these employees showed significant personal use.

Employees' personal use included accessing websites related to personal shopping, online banking, bill paying, personal email, entertainment, social media and web searches for non-District related subjects. One employee with significant personal Internet use also used her official District email address for herself and a family member to subscribe to retailers and other entities unrelated to District business. Another District official used the District's IT resources to conduct her own personal business, such as creating shipping labels for items she sold at an online marketplace or organizing promotional events to sell non-District related items. One IT employee, with administrative permissions to make system-wide changes, also told us that he regularly brought his laptop computer home and allowed his family members to use this device. We found that this computer was infected with malware.

We further found that nine of 10 employees in our sample, including all eight employees with personal Internet use, had signed AUPs in their personnel files indicating they received, read and understood the AUP's requirements. The Superintendent was the only employee without a signed AUP in his personnel file.

Although officials told us they use a web filter and that the CNYRIC monitors its firewall, officials did not take the additional steps that would be needed to detect or prevent these personal Internet activities. Internet browsing increases the likelihood of computers being exposed to malicious software that may

Although officials told us they use a web filter and that the CNYRIC monitors its firewall, officials did not take the additional steps that would be needed to detect or prevent these personal Internet activities.

compromise PPSI. An employee could unknowingly open a malicious email attachment, download a malicious file from the Internet or visit an infected website. As a result, the District's IT assets and any PPSI they contain have a higher risk of exposure to damage and PPSI breach, loss or misuse. Additionally, when employees use District resources for non-District activities, productivity may be reduced.

Why Should the District Properly Manage Network User Accounts and Permissions?

District officials are responsible for restricting user access to only those resources and data needed for learning and to complete job duties and responsibilities. This restriction helps ensure data and IT assets are protected from unauthorized use and/or modification.

Network user accounts provide access to resources on a network and user computers. These accounts are managed centrally by a server and/or domain controller. Network resources include those on networked computers, such as shared folders, and in certain applications, such as an email application. A domain controller is the main server in the domain (network) that controls or manages all computers within the domain.

A district should have written procedures for granting, changing and disabling user permissions to the network. To minimize the risk of unauthorized access, district officials should actively manage network user accounts, including their creation, use and dormancy, and regularly review enabled network accounts to ensure they are still needed. When employees leave district employment, or when user accounts are otherwise no longer needed, officials should ensure that these accounts are disabled in a timely manner.

Generic accounts are not linked to individual users and may be needed for certain network services or applications to run properly. For example, generic accounts can be created and used for automated backup or testing processes, training purposes or generic email accounts, such as a service helpdesk account. Officials should also routinely evaluate generic network user accounts and disable those that are not related to a current district or system need.

A shared account is an account with a username and password that is shared among two or more people. Because shared accounts are not assigned to a single user, officials may have difficulty linking any suspicious activity to a specific user. To help ensure individual accountability, all users should have and use their own user account to gain access to a network. If shared accounts are needed, officials should have procedures in place to monitor who uses the accounts and when they are used. This helps ensure accountability over work performed and data changed or deleted.

Generally, an administrative account has permissions to monitor and control networks and computers, including the ability to add new users and change user passwords and permissions. A user with administrative permissions can make system-wide changes, including installing programs of his/her own choosing and manipulating settings configured for security purposes. As a result, officials must limit administrative permissions to only those users who need them to perform their job functions and responsibilities.

When users have unneeded administrative permissions to a network, they could make unauthorized changes that might not be detected. In addition, the misuse of administrative permissions is a method often used by attackers to compromise or disrupt systems.

A user can be deceived into opening a malicious email attachment, downloading and opening a file from a malicious website or accessing a website programmed to automatically infect the user's computer with malicious software. If the deceived user has administrative permissions, an attacker could use those elevated privileges to cause greater damage than with a lesser-privileged account.

Officials Did Not Adequately Manage Network User Accounts and Permissions

District officials did not adequately manage network user accounts and permissions for the District Office network. Officials did not have written policies or procedures for managing user accounts and permissions. They told us that when an employee was terminated or otherwise left the District's employment, the District Clerk would inform the IT department, authorizing the department to modify or disable the employee's network user account. Prior to disabling the account, the IT department would leave the account enabled for an indefinite time so that the employee could access any necessary files. Therefore, the District Office network had unnecessary user accounts enabled. Because officials did not have a written user account management policy to provide guidance to employees and IT personnel, unneeded network user accounts and accounts with unnecessary administrative permissions went unnoticed until our audit.

We examined all 31 enabled network user accounts on the District Office domain controller to determine whether any were unneeded accounts or accounts with unneeded administrative permissions.

<u>Unneeded Network User Accounts</u> − We found six (19 percent) enabled, active network user accounts that were assigned to former employees or third-party consultants who no longer provided service to the District. Of these, four had never been used to log onto the network and one was last used in August 2019. The Director told us she would disable or delete the unneeded network user accounts we identified.

Unneeded network user accounts can be potential entry points for attackers and could be used to inappropriately access and view PPSI.

Shared Accounts − We found seven (23 percent) shared, generic network user accounts that had varied purposes, such as accounts for third-party consultants to provide IT support to the District and an account to test and troubleshoot virtual private network connections. Of the seven, District officials told us three were unnecessary. District officials also told us that the District did not have procedures in place to monitor who used any of these shared accounts, when they were used or for what purpose.

When a number of employees and external consultants share an account without procedures for monitoring the use of the account, the District has a greater risk that PPSI could be changed intentionally or unintentionally or used inappropriately, and officials would not be able to identify who performed the unauthorized activities.

Administrative Permissions − We found eight (26 percent) network user accounts with administrative permissions. Three of these accounts were no longer needed, as two were assigned to individuals who were no longer associated with the District, and one was a duplicate of an existing generic user account. District officials did not have a reason for not promptly disabling these unneeded accounts and their administrative permissions.

A compromised network user account with administrative permissions could result in greater damage than with a lesser-privileged account, including unauthorized manipulation of data or disruption of District operations.

Why Should the District Provide IT Security Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, district officials should provide periodic IT security awareness training. This training should explain the proper rules of behavior for using the Internet, IT systems, data and PPSI. The training also should communicate related policies and procedures to all employees using IT resources and explain the consequences of policy violations. The training should center on emerging trends such as information theft, social engineering attacks (methods used to deceive users into revealing confidential or sensitive information) and computer viruses, and other types of malicious software, all of which may result in PPSI compromise or expose the district to ransomware attacks.

Training programs should be directed at the specific audience (e.g., system users or administrators) and include everything that attendees need to perform their jobs. Training programs should also cover key security concepts, such as the dangers of Internet browsing and downloading files and programs from the

Internet, requirements related to protecting PPSI, the importance of selecting strong passwords, and how to respond if a cyber incident is detected.

Officials Did Not Provide IT Security Awareness Training to District Staff

As of the end of our audit fieldwork in December 2020, the District had not provided employees with any formalized IT security awareness training to ensure they understood security measures needed to protect the network. The Director occasionally sent out emails to keep employees informed about known or possible IT cyberattacks and proper use of the District's computer system; however, those emails were not a sufficient substitute for formal IT security awareness training. We found that two District employees attempted to download and install unapproved software/applications from the Internet, suggesting that users may have insufficient understanding of the proper security measures required while using the District's IT resources.

The District subscribed to the CNYRIC's service to provide formal IT security awareness training to its employees for the 2020-21 school year. However, at the time of our fieldwork, the Director told us the training was not yet implemented. The Director later told us that trainings on topics such as data security, privacy, phishing scams, malware and password practices, are planned for Spring 2021.

The IT cybersecurity community identifies end-users as the weakest link in the chain to secure data and IT systems. District officials cannot protect the confidentiality, integrity and availability of data and computer systems without ensuring that employees understand their roles and responsibilities related to IT and data security. Without periodic, formal security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise IT assets. As a result, data and PPSI could be at greater risk for unauthorized access, misuse or abuse.

The IT cybersecurity community identifies end-users as the weakest link in the chain to secure data and IT systems.

What Do We Recommend?

District officials should:

1. Ensure all officials and employees who use District IT resources sign and return the AUP.
2. Develop written procedures for changing and revoking staff's access rights to the network accounts.
3. Provide employees with periodic, formal IT security awareness training that reflects current risks identified by the IT community.

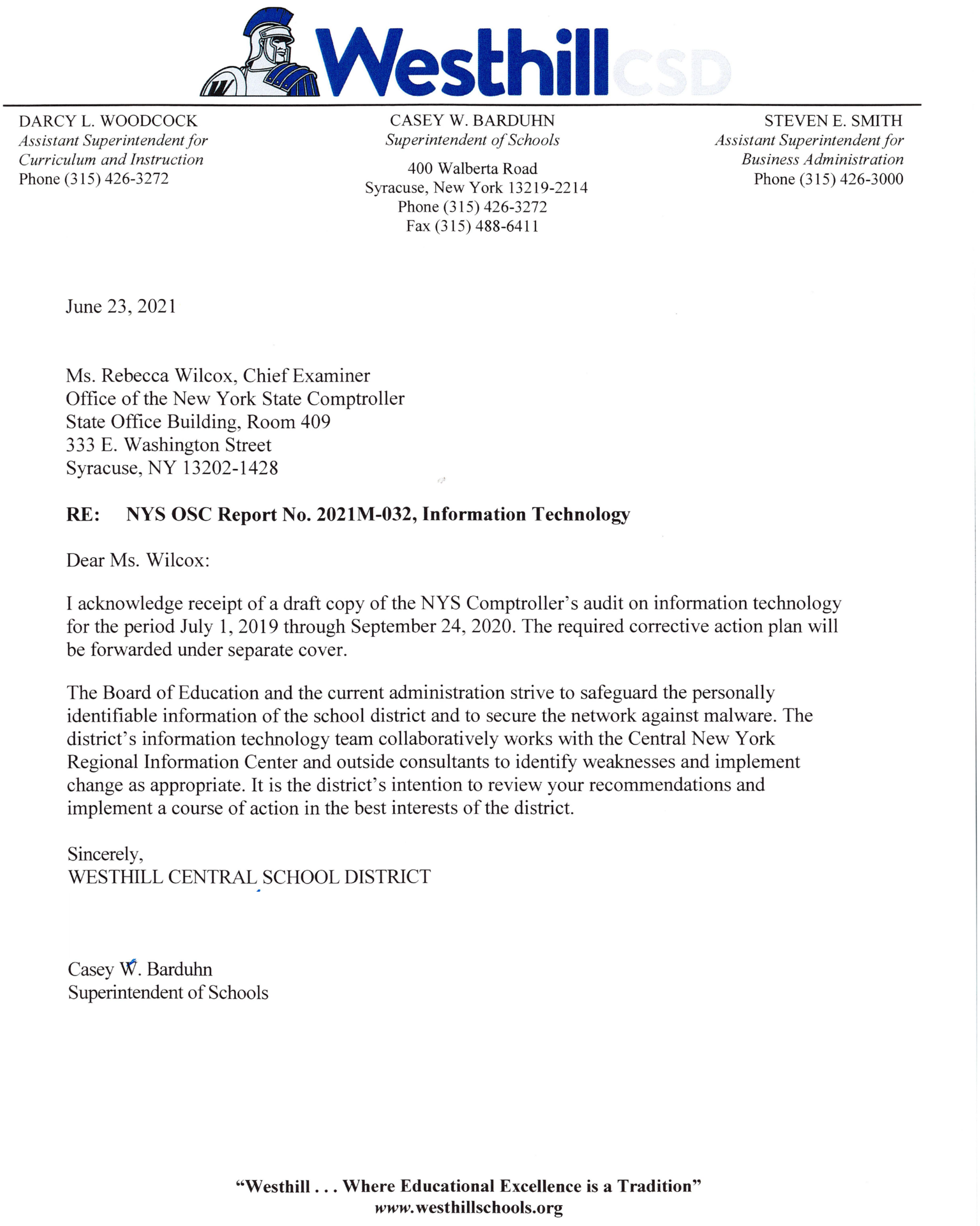
The Director should:

4. Monitor employee computer use to ensure compliance with the AUP.

5. Disable network accounts of employees and consultants as soon as they leave District employment, and routinely review network user accounts and disable those that are no longer needed.

6. Restrict the use of shared network user accounts and develop procedures to monitor the use of these accounts.

Appendix A: Response From District Officials



Westhill CSD

DARCY L. WOODCOCK
Assistant Superintendent for
Curriculum and Instruction
Phone (315) 426-3272

CASEY W. BARDUHN
Superintendent of Schools

400 Walberta Road
Syracuse, New York 13219-2214
Phone (315) 426-3272
Fax (315) 488-6411

STEVEN E. SMITH
Assistant Superintendent for
Business Administration
Phone (315) 426-3000

June 23, 2021

Ms. Rebecca Wilcox, Chief Examiner
Office of the New York State Comptroller
State Office Building, Room 409
333 E. Washington Street
Syracuse, NY 13202-1428

RE: NYS OSC Report No. 2021M-032, Information Technology

Dear Ms. Wilcox:

I acknowledge receipt of a draft copy of the NYS Comptroller's audit on information technology for the period July 1, 2019 through September 24, 2020. The required corrective action plan will be forwarded under separate cover.

The Board of Education and the current administration strive to safeguard the personally identifiable information of the school district and to secure the network against malware. The district's information technology team collaboratively works with the Central New York Regional Information Center and outside consultants to identify weaknesses and implement change as appropriate. It is the district's intention to review your recommendations and implement a course of action in the best interests of the district.

Sincerely,
WESTHILL CENTRAL SCHOOL DISTRICT

Casey W. Barduhn
Superintendent of Schools

"Westhill . . . Where Educational Excellence is a Tradition"
***www.*westhillschools.org**

Appendix B: Audit Methodology and Standards

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We interviewed District officials and employees and reviewed the District's policies to gain an understanding of the District's IT internal controls.
- We used our professional judgment to select a sample of 12 District computers assigned to 10 employees. We chose these employees because they had either administrative access to the network and IT system or access to financial and employee records. We ran computerized audit scripts on the computers to review web histories and evaluate whether their Internet browsing use was in compliance with the AUP. Because web history data from one computer was incompatible with our conversion and analysis tool, we reduced our testing of web histories to 11 computers.
- We used a computerized audit script to examine the District Office's domain controller and analyzed the data produced to assess network user accounts, permissions assigned to these accounts and the related security settings applied to the accounts. We compared all 31 enabled network accounts on the District Office's domain controller to the active employee list to identify accounts for former employees and/or unneeded accounts.

Our audit also examined the adequacy of certain information technology controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to District officials.

We conducted this performance audit in accordance with 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.

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.

The Board has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law, Section 2116-a(3)(c) of New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the 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 CAP should be posted to District's website for public review.

Appendix C: Resources and Services

Regional Office Directory
https://www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
https://www.osc.state.ny.us/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
https://www.osc.state.ny.us/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
https://www.osc.state.ny.us/files/local-government/publications/pdf/cyber-security-guide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
https://www.osc.state.ny.us/local-government/publications

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

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

www.osc.state.ny.us/local-government

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

SYRACUSE REGIONAL OFFICE – Rebecca Wilcox, Chief Examiner

State Office Building, Room 409 • 333 E. Washington Street • Syracuse, New York 13202-1428

Tel (315) 428-4192 • Fax (315) 426-2119 • Email: Muni-Syracuse@osc.ny.gov

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

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