REPORT OF EXAMINATION | 2020M-106

Dryden Central School District

Information Technology

FEBRUARY 2021

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

Contents

Report Highlights

Dryden Central School District

Audit Objective

Determine whether the Dryden Central School District's (District) Board of Education (Board) and District officials adequately safeguarded personal, private and sensitive information (PPSI) from abuse or loss.

Key Findings

The Board and District officials did not adequately safeguard PPSI. Officials did not:

- Ensure information technology (IT) policies were up-to-date with current technology changes, existing policies were enforced (or enforceable).
- Regularly review user accounts and disable any unnecessary accounts, maintain up-to-date IT asset inventory records or enter into adequate written contracts with all IT service providers.

In 2018, the District was the victim of a ransomware attack. The Director of Information Technology Services (IT Director) failed to determine whether any data was taken or notify either those affected by the security breach or the Board and Superintendent of the attack.

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

Key Recommendations

- Review and modify IT policies to ensure they are enforceable within their IT environment.
- Evaluate all existing user accounts, periodically review for necessity and appropriateness, and adequate written contracts are entered into with all IT service providers.

District officials agreed with our recommendations and indicated they will take corrective action.

Background

The District serves three towns in Tompkins County, two towns in Cortland County and one town in Tioga County. The District is governed by an elected nine member Board. The Board is responsible for the general management and control of financial and educational affairs.

The Superintendent of Schools (Superintendent) is the District's chief executive officer and is responsible, along with other administrative staff, for day-to-day management under the Board's direction.

The District's Director of Information Technology Services (IT Director) is responsible for managing the District's IT operations and reports to the Superintendent and Board. The District contracts with the Central New York Regional Information Center (RIC) and the Tompkins-Seneca-Tioga Board of Cooperative Educational Services (TST BOCES) to provide IT services.

Quick Facts	
Desktops, Laptops and Other Devices	3,233
Total Enabled Network User Accounts	1,745
Enabled Non-student Network Accounts	561

Audit Period

July 1, 2018 - January 31, 2020

Information Technology

The District's IT systems and data are valuable resources. The District relies on its IT assets for a variety of tasks, including Internet access, protecting personal, private and sensitive information (PPSI),[1] email and maintaining financial, personnel and student records.

The District was the victim of a ransomware attack in 2018.[2] The ransomware program encrypted and locked District files rendering the files and information inaccessible. During that period of time the information was no longer in District control, which could be considered a security breach, as defined by the District's information security breach and notification policy.

District officials did not implement effective controls to reduce the risk of another such attack in the future. While effective controls will not guarantee the safety of a computer system, a lack of effective controls significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use, and increases the likelihood of another attack.

Why Should the Board Review and Periodically Update IT Policies?

IT security policies describe the tools and procedures to protect PPSI and information systems, define appropriate user behavior and explain the consequences of policy violations. A board must establish security policies for all IT assets and information, disseminate the policies to officials and staff and ensure that officials monitor and enforce the policies.

Policies that should be established include, but are not limited to, acceptable computer use, data network and security access, information security breach and notifications, and Internet safety/Internet content filtering. In addition, New York State Technology Law requires districts to notify affected individuals when there is a system security breach involving personal information.[3] All policies should include who is responsible for monitoring and enforcing the policies, how to monitor and enforce the policies and the possible disciplinary action that will be taken for violation of the policies.

Because technology terminology and usage is ever changing, it is important that the board periodically review adopted policies to ensure they remain current and the IT director be involved in any policy development or modification that relates to the district's IT environment. Any policy requirements should consider the current network infrastructure and be adapted so implementation is feasible.

---

1 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, third-parties or other individuals or entities.

2 Ransomware is a type of malicious software that prevents users from accessing their computer systems or electronic data until a ransom payment is made.

3 New York State Technology Law, Section 208

The Board Did Not Review and Periodically Update IT Policies

While the Board adopted the recommended policies, it failed to ensure that policies were reviewed and periodically updated or involve the IT Director in any policy development or modification related to the District's IT environment.

We reviewed the adoption and revision dates of all District policies and found some have not been revised in as long as 10 years (Figure 1).

Figure 1: Board-Adopted IT Policies and Revisions

Title	Date of Adoption	Date of Last Revision
Information Security Breach and Notification	01/26/09	Being Revised
Employee Personal Identifying Information	06/22/09	None Since Adoption
Data Network and Security Access	06/08/15	None Since Adoption
Student Grading Information System	06/08/15	None Since Adoption
Staff Use of Computerized Resources	01/26/09	01/13/14
Use of Email in District	01/26/09	01/13/14
Student-Staff Acceptable Use Policy	06/25/07	None Since Adoption
Student Data Breaches	01/26/09	None Since Adoption
Internet Safety/Internet Content Filtering	01/26/09	04/16/12

During our meeting with the IT Director, she told us that the District was the victim of a ransomware attack in 2018. The ransomware program encrypted and locked District files rendering the files and information inaccessible. During that period of time the information was no longer in District control, which could be considered a security breach, as defined by the District's information security breach and notification policy. The policy defines a breach of system security as any "… unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the District."

The IT Director said that the only step taken to address the attack was to restore backups of the affected servers. However, she did not determine whether any data was taken or if the attack required any of the directives outlined in the policy to be followed. Therefore, parents, students, or other owners/residents whose data was potentially effected were not notified of the attack. Furthermore, the Board and Superintendent were unaware of the attack until we discussed the breach with them during our audit.

Further, other District policies were either not enforced or unenforceable based on current network configurations, including the computer hardware and software used.

- The student-staff acceptable use policy requires the use of a particular web browser. However, this browser was specific to an operating system that cannot be run on a significant number of the District's laptops. Because officials did not update this policy, most internet access was a violation of the policy.
- The staff use of computerized resources policy states that staff must sign an acceptable use acknowledgment form annually and the form will be maintained in the employee personnel files. We reviewed the personnel files for 26 employees. We found that two files had no acknowledgments and 19 had acknowledgments signed and dated before 2019, including the Superintendent's acknowledgment that was signed in 2012.
- The data network and security access policy contains 11 directives. However, we found that officials were not enforcing seven of them (64 percent). For example, officials did not prepare an inventory and classification of PPSI or effectively prepare accurate, up-to-date inventories of IT assets.
- The Internet safety/Internet content filtering policy states that appropriate District personnel will be present when students access the Internet. However, this is no longer true or practical because students have access to the Internet using District provided laptops from their homes.

Officials told us that they contract with another BOCES for policy development, which provides templates of policies and notifies the District when policies may need to be updated or modified based on changes to State, federal or other governing board's laws or regulations.

We compared the District's IT policies to two neighboring districts' policies and found that seven policies were identical to those at one district and six were identical to the other district, indicating that District officials were adopting the templated policies from BOCES as their own. Without considering edits or modifications to these templates, officials have adopted policies that either do not meet the needs of the District's IT environment or are unenforceable because of the District's IT environment.

While IT policies do not guarantee the safety of the District's computer system or the PPSI and electronic information contained therein, the lack of updated enforceable policies significantly increases the risk that data, hardware and software systems may be lost or damaged by inappropriate access and use and increases the likelihood of another ransomware attack. Without comprehensive policies that explicitly convey the appropriate use of the District's computer equipment, the IT Director's involvement in policy development or modification and practices to safeguard data, officials cannot ensure employees are aware of their responsibilities.

Why Should Officials Properly Manage User Accounts?

Network user accounts provide access to network resources and should be actively managed to minimize the risk of misuse. If not properly managed, network user accounts could be potential entry points for attackers because they could be used to inappropriately access data and view PPSI on the network.

A district should have written procedures granting, changing and revoking user access to its network. To minimize the risk of unauthorized access, officials should regularly review enabled network accounts to ensure they are still needed and that user account access is appropriate to fulfill their job duties and responsibilities. Officials should disable unnecessary accounts as soon as there is no longer a need for them.

Generic accounts are used by certain network services to run properly and can be created for services that are not linked to a personal account to meet various business needs. For example, generic accounts can be used for classroom instructional purposes or to scan student tests. Officials should routinely evaluate and disable any generic accounts that are not related to a specific system need.

Officials Did Not Properly Manage User Accounts

The District's IT Director is the network administrator and is responsible along with other IT staff for overseeing the District's network. Officials told us that one staff member was responsible for adding, modifying and disabling network user accounts. This staff member generally received an email from the human resource department including a copy of the Board minutes authorizing the hiring or resignation of staff members.

Based on this notification, the staff member would make the necessary changes for the particular user. She also periodically reviewed Board minutes to ensure she was aware of all new hires or resignations. In some rare instances, various officials would verbally tell her to add or disable network user accounts.[4]

We examined all 561 enabled non-student network user accounts and found the following:

- 82 network user accounts did not match the list of current employees. Officials did not provide us with an explanation for 10 of these accounts or the users' relationship to the District. The IT Director told us that all but one account was disabled after we provided her the list of non-employee accounts. The IT Director said that this account was for a student teacher. However, officials were unable to provide us with documentation to show that this individual ever worked at the District.

4 These officials included the Human Resource Director, IT Director, Business Manager and Board Clerk.

- 17 network accounts were disabled after we provided a list to officials showing that these accounts were no longer needed and should have been disabled before we brought it to their attention.

In addition, we identified 108 generic accounts and did not receive an explanation from officials for the need or use of these accounts. We questioned whether 65 generic accounts were still needed based on the frequency of use:

- 32 accounts had never been used.
- 11 classroom accounts had not been used in three to seven years.
- 4 built-in accounts had not been used in two to 10 years.
- 4 test accounts had not been used in four to 10 years.
- 14 accounts for various uses were not readily explainable and had not been used in 7 months to 10 years.

District officials acknowledged that they did not have a formal process to ensure only necessary employee and non-employee network user accounts were active. Because the District did not have formal procedures for revoking access permissions and regularly reviewing enabled user accounts, the unneeded user accounts and permissions went unnoticed until our audit.

In addition, because the District's network had unused, unneeded active unused network and generic user accounts, it had a greater risk that these accounts could have been used as entry points for attackers to access PPSI and compromise IT resources.

District officials… did not have a formal process to ensure only necessary… user accounts were active.

Why Should Officials Maintain Accurate, Up-To-Date IT Inventory Records?

Computer equipment management is essential to safeguarding district assets, PPSI and data. District officials should maintain detailed, up-to-date inventory records for all computer hardware to safeguard IT assets. Reliable IT inventory records are critical for protecting these assets from loss or misuse. District officials cannot properly track and protect IT assets if they do not know what IT assets they have and where those assets reside. The failure to maintain detailed, up-to-date inventory exposes these valuable assets to an increased risk of loss, theft or misuse, putting district data and PPSI at risk.

Information maintained for each piece of computer equipment should include a description of the item, name of the employee to whom the equipment is assigned, physical location of the equipment and relevant purchase or lease information. Officials should verify the accuracy of inventory records through periodic physical inventory counts.

Officials Did Not Maintain Accurate, Up-To-Date IT Inventory Records

Officials did not maintain accurate, detailed up-to-date inventory records of all IT equipment. The District's data network and security access policy required the Superintendent or the IT Director, as the Superintendent's designee, to identify all new IT equipment when it was purchased, periodically perform physical inventory checks and update the inventory list. Currently, officials maintain the IT equipment inventory using three different software programs that have inventory tracking capabilities and each track specific types of IT equipment.

District IT staff told us that IT assets were not immediately added to inventory when purchased as dictated by District policy. Instead IT assets were added to the appropriate inventory list after it had been set up for use and delivered to its assigned individual.

Further, the IT Director told us that an annual physical inventory of IT equipment is conducted on all IT equipment over the summer months when the equipment is cleaned. However, she said not all equipment was cleaned or counted during the summer of 2019. For example, none of the business office's IT equipment was cleaned or counted that year because staff was using the equipment. In addition, the laptops that many students took home for the summer were not cleaned or included in the physical inventory count.

We found that 798 of the 3,233 items on the inventory report did not include a physical location for the asset and 110 of these items did not have affixed identification numbers. Furthermore, when we compared the inventory records to recent lists of equipment disposals, we found that 11 disposed-of items remained on the list.

The District cannot properly protect IT resources if personnel are unaware of existing resources and where they reside. Because officials did not maintain accurate, detailed, up-to-date inventory records, the District had an increased risk that its IT assets may be lost, stolen or misused. Furthermore, any PPSI stored or located on the equipment is not protected from unauthorized access or use.

Why Should Officials Have Written IT Contracts and Service Level Agreements (SLA)?

A written contract provides both parties with a clear understanding of the services expected to be provided and a legal basis for compensation provided for those services. A board should have a formal written contract with its IT provider that indicates the contract period, services to be provided and basis of compensation for those services. In addition, to protect the district and avoid potential misunderstandings, officials should have a separate written SLA between the district and its IT consultant that identifies the district's needs and expectations and specifies the level of service to be provided by the IT consultant.

An SLA is different from a traditional written contract because it establishes comprehensive, measureable performance targets so that there is a mutual understanding of the nature and required level of services to be provided. It provides detailed explanations of the services to be performed by identifying the parties to the contract and defining terminology; term or duration of the agreement; scope and/or subject limitations; service level objectives; performance indicators; roles and responsibilities; nonperformance impact; security and audit procedures; reporting requirements; review, update and approval process; and pricing, billing and terms of payment.

The District Did Not Have Adequate IT Contracts and SLAs

The District paid the RIC and TST BOCES more than $300,000 to provide IT related services in 2018-19. We found that District officials did not have contracts with either the RIC or TST BOCES detailing the roles and responsibilities for all parties involved.

Officials provided us with various cooperative service agreement (COSER) descriptions for the IT services available from the RIC that did not state which of these services the District was receiving, provide any detailed information for services to be provided, explain District and RIC responsibilities or include comprehensive measurable performance targets. As a result, the document was not as detailed as an SLA should be. TST BOCES provided even less information in their COSER. The District received a quarterly bill for all services TST BOCES provided under each COSER and the amount owed for that service, with IT services listed on the bill.

We contacted the RIC and asked about the backup procedures for District data and were told that the RIC does weekly and monthly back-ups of District data.[5] However, the RIC did not provide any reports of these back-ups to the District including what data was included or whether the back-ups were successful. RIC personnel told us that back-ups are periodically tested (restored) but no reports of the success or failure of the testing was provided to the District. We also contacted TST BOCES for an SLA and did not receive a response.

Without adequate written contracts and SLAs, District officials did not have a documented understanding of the services expected to be provided by the RIC or TST BOCES. In addition, the District did not have contractual or legal protection if the RIC or TST BOCES defaulted on their obligations. As a result, the District had a greater risk that its computer resources and PPSI could have been accessed by attackers, misused or abused.

5 A backup is a copy of data files and software programs made to replace original versions if there is loss or damage to the original.

Why Should the Board Adopt a Detailed Disaster Recovery Plan?

A disaster recovery plan provides a framework for reconstructing vital operations to resume time-sensitive operations and services after a disaster. Disasters may include any sudden, unplanned catastrophic event (e.g., fire, flood, computer virus or inadvertent employee action) that compromises the availability or integrity of district services, including the IT system and data.

Typically, a disaster recovery plan includes an analysis of business processes and continuity needs, disaster prevention instructions, specific roles of key individuals and precautions needed to maintain or quickly resume operations. Additionally, a disaster recovery plan should include data backup procedures and periodic backup testing to ensure they will function as expected.

A disaster recovery plan provides a framework for reconstructing vital operations to resume time-sensitive operations and services after a disaster.

The Board Did Not Adopt a Disaster Recovery Plan

The Board did not adopt a comprehensive disaster recovery plan to address potential disasters. When we discussed the importance of a disaster recovery plan with officials, they started to draft a plan.

However, without a formal written plan, the District has an increased risk that it could lose important data and suffer a serious interruption to operations, such as not being able to process checks to pay vendors or employees or process grades and State aid claims.

While we commend officials for starting to develop a plan, we encourage them to finish the development and adopt their plan.

What Do We Recommend?

District officials should:

1. Review and modify policies to ensure adopted policies are enforceable within their IT environment and periodically review the policies to ensure they remain current with emerging technologies.
2. Ensure there are adequate written contracts and SLAs with all parties providing IT services to the District that include a schedule of reports or other services to be provided to will help ensure an understanding of all services to be provided and the roles and responsibilities of each party.
3. Continue to develop and adopt the written disaster recovery plan.

The IT Director should:

4. Evaluate all existing network user and generic accounts, disable any deemed unnecessary and periodically review for necessity and appropriateness.

5. Ensure that up-to-date inventory records are maintained and that physical inventories are performed at least annually.

Appendix A: Response From District Officials

DRYDEN
CENTRAL SCHOOL DISTRICT

January 15, 2021

Office of the State Comptroller
Attn: Ann Singer, Chief Examiner
State Office Building, Room 1702
44 Hawley Street
Binghamton, New York 13901-4417

Subject: Response to Preliminary Draft Audit Findings

Dear Ms. Singer,

This letter is the Dryden Central School District's response to the draft audit report into information technology covering the period of 01-JUL-2018-31-JAN-2020. I am pleased to say that the audit was a fair examination of the District's information technology's policies, protocols, and procedures. The District's Leadership Team and Board of Education believes in continuous improvement of our operations in order for us to become more efficient and better serve our students, staff, and community.

Recommendation 1: The District should review and modify policies to ensure adopted policies are enforceable within their IT environment and periodically review the policies to ensure they remain current with emerging technologies.

District Response: The Dryden Central School District agrees with the audit finding and recognizes its importance that relevant, updated and enforceable IT policies play in ensuring safety and privacy as well as limiting exposure and liability of the District. Our corrective action plan will outline the specific steps that the District is taking to review, update, and amend current policies as well as develop additional policies that support the spirit of Recommendation 1. The District has a contract with Erie 1 BOCES to help develop policy. Many of the District's current policies are based on the guidance and support we have received from Erie1.

Recommendation 2: Ensure there are adequate written contracts and SLAs with all parties providing IT services to the District that include a schedule of reports or other services to be provided to will help ensure an understanding of all services to be provided and the roles and responsibilities of each party.

District Response: The Dryden Central School District agrees with the audit finding and recognizes the importance of these SLAs and written contracts play in a strong IT Department. In addition, the District understands the importance that these agreements play in protecting the District. The District uses the CNYRIC and BOCES to support many functions related to IT and these agreements and schedules have not been provided to LEAs in the past. Our corrective action plan will address a plan to secure these contracts and agreements moving forward.

#Lion Pride

PO Box 88, Dryden, NY 13053 | Phone 607.844.8694 | Fax 607.844.4733

DRYDEN
CENTRAL SCHOOL DISTRICT

Recommendation 3: Continue to develop and adopt the written disaster recovery plan.
District Response: The Dryden Central School District agrees with the audit finding and our corrective action plan will detail a timeline to develop this plan for BOE adoption.

Recommendation 4: The IT Director should evaluate all existing network user and generic accounts, disable any deemed unnecessary and periodically review for necessity and appropriateness.

District Response: The Dryden Central School District agrees with the audit finding and the Superintendent and IT Director will develop a timeline to ensure this Recommendation is addressed. The timeline along with benchmark outcomes will be outlined in the forthcoming Corrective Action Plan.

Recommendation 5: The IT Director will ensure that up to date inventory records are maintained and that physical inventories are performed annually.

District Response: The Dryden Central School District agrees with the audit finding and the Superintendent and IT Director will develop a timeline to ensure this Recommendation is addressed. The timeline along with benchmark outcomes will be outlined in the forthcoming Corrective Action Plan. In addition, the Superintendent and the IT Director will develop an annual schedule to ensure that the inventory is consistently and accurately updated.

Respectfully submitted,

Joshua I. Bacigalupi
Superintendent of Schools

#Lion Pride

PO Box 88, Dryden, NY 13053 | Phone 607.844.8694 | Fax 607.844.4733

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 IT staff members to obtain an understanding of the District's IT operations including the safeguards to protect sensitive data, the existence and testing of a disaster recovery plan and whether any employees received IT security awareness training and what that training consisted of. We also conducted interviews with staff from the RIC and TST BOCES to gain an understanding of the services they are providing to the District.
- We obtained and reviewed the adoption and revision dates of the Board policies related to IT to determine the length of time since policies were reviewed and revised. We also reviewed the policies to determine if language was enforceable considering the technology described in the policies versus the District's current IT environment. Finally, we compared the District's policies to three neighboring districts' policies to determine whether the Board adopted templated or customized policies.
- We reviewed the steps the IT Director took to determine whether provisions in the information security breach and notification policy were followed including notifying the Superintendent and Board of the ransomware attack.
- We used specialized audit software to review all 561 non-student user accounts and compared them to the current employee list to identify inactive and unneeded accounts. We also analyzed user accounts and security settings applied to those accounts on the District servers.
- We discussed inventory controls with the IT Director and staff to determine the processes and procedures followed regarding inventory. We obtained the District's IT inventory records and compared them to disposal records to determine whether inventory records were accurate and up-to-date.
- We reviewed contractual documents between the District and RIC and TST BOCES to determine the IT services to be provided, reporting requirements, performance indicators and security procedures.

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 2116-1(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 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 the District's website for public review.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/sites/default/files/local-government/documents/pdf/2018-12/regional_directory.pdf

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

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

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263206&issued=All

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

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/sites/default/files/local-government/documents/pdf/2020-05/cyber-security-guide.pdf

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

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263211&issued=All

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

Contact

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

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

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

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

BINGHAMTON REGIONAL OFFICE – Ann C. Singer, Chief Examiner

State Office Building, Suite 1702 • 44 Hawley Street • Binghamton, New York 13901-4417

Tel (607) 721-8306 • Fax (607) 721-8313 • Email: Muni-Binghamton@osc.ny.gov

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

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