

Building Access in Schools



Prepared by the Division of Local Government and School Accountability

Table of Contents

Executive Summary	1
Building Access	2
School officials did not ensure all building access accounts and devices were needed.	2
The Schools had inadequate, outdated or no building access account monitoring procedures.	5
Best practices we observed	6
Conclusion	6
Appendix A: Background and Relevant Standards	7
Additional Resources	8
Appendix B: Selected Schools – Accounts and Devices Reviewed	9
Notes	10

Executive Summary

School districts and Boards of Cooperative Educational Services (BOCES) (together “schools”) are responsible for developing and maintaining a safe environment for their students, staff, and visitors. As a cornerstone for communities and often settings for the most formative experiences in a child’s life, it is crucial that schools are safe and secure to provide an optimal educational environment for students and staff.

Properly managing and monitoring building access is a fundamental security function and the responsibility of school officials. Building access management systems (systems) are designed to regulate entry and exit points, allowing authorized individuals to access buildings or specific areas while keeping unauthorized individuals out. Improper management and monitoring of building access can compromise security by allowing unauthorized individuals, including those without appropriate background checks, to gain access to school buildings and students.

We selected 20 schools¹ (Schools) to determine whether the Schools’ officials properly managed and monitored building access accounts (accounts) and devices. The Schools used various systems for access control and monitoring (e.g., key fobs, keycards, badges) issued to current employees as well as non-employees (i.e., first responders,² vendors, contractors, etc.), including shared devices.³

We visited the Schools between December 2025 and May 2026 and identified that officials did not disable all unneeded building access accounts and devices. Of the 17,195 devices that were active at the time of the audits, we identified 1,564 (9 percent) that were unneeded, the majority of which (65 percent) were non-employee devices, including shared devices. Specifically, of the accounts and devices we reviewed:

- All 20 Schools (100 percent) had unneeded active accounts and devices.
- 19 Schools (95 percent) did not properly monitor and track shared devices.
- 18 Schools (90 percent) had employees with duplicate active devices.
- 12 Schools (60 percent) did not have any written policies and procedures outlining who is responsible for managing and monitoring accounts.
- 10 Schools (50 percent) had non-employees with duplicate active devices.

Officials at all 20 Schools can improve how they manage accounts and devices. As a result, because accounts and devices were not properly managed and monitored, there were potential risks for unauthorized access to the Schools’ buildings, compromising building security and safety for students, teachers, staff and visitors.

This report is a compilation of audit work performed under generally accepted government auditing standards (GAGAS). The scope of this report on its own does not constitute an audit under GAGAS. For further information about the Schools, including their active accounts and devices, results of testing and links to the Schools’ audit reports,⁴ see Appendix B.

Building Access

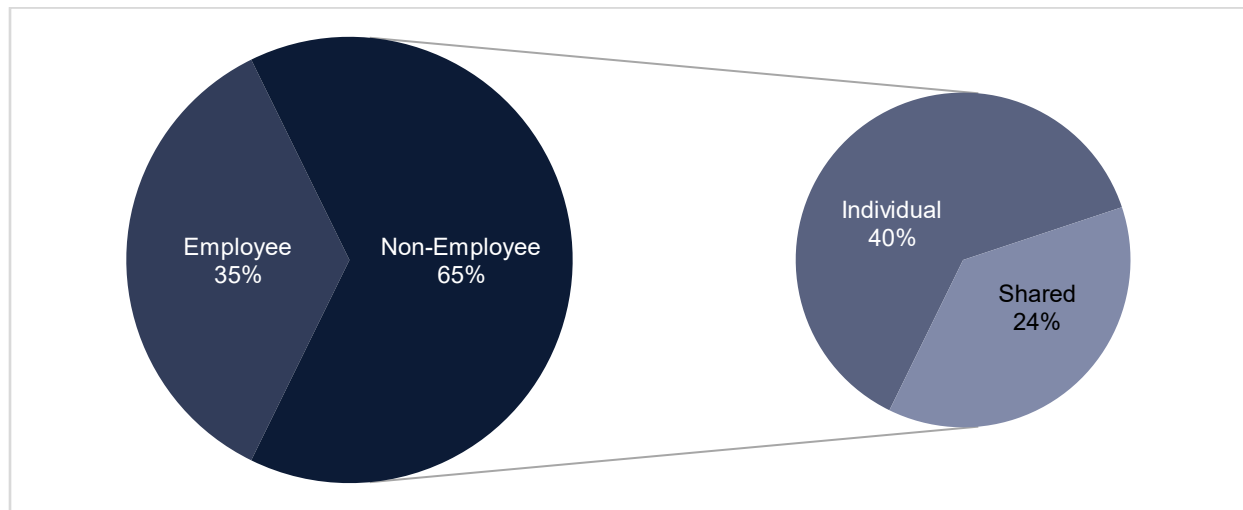
Building access controls are essential for enhancing security and enabling school officials to manage and monitor entry points within educational institutions. These systems authenticate an individual or user through devices such as key fobs, keycards, badges, or similar technologies, helping to ensure only authorized individuals can enter school buildings. By limiting access this way, schools can better safeguard their facilities and maintain a safe and secure environment for students, teachers, staff and visitors.

The relevant standards, resources and publications we used in our review are included in Appendix A.

School officials did not ensure all building access accounts and devices were needed.

At the 20 Schools, we identified a total of 17,195 devices with 12,042 devices issued to current employees, and 5,134 devices issued to non-employees including 1,975 shared devices. Of the 17,195 active devices, we identified 1,564 active but unneeded devices within the 20 Schools' systems, the majority of which (65 percent) were non-employee devices, including shared devices (Figure 1).

Figure 1: Unneeded Devices



These unneeded active devices were not disabled when no longer needed.

Duplicate Devices – 18 Schools (90 percent) had employees with two or more active devices, including one School where an employee had as many as seven active devices, and 10 Schools (50 percent) issued two or more active devices to non-employees. In total, of the accounts and devices we reviewed, there were 555 duplicate employee devices issued to 498 employees, and 129 duplicate devices issued to 117 individual non-employees.

These duplicate devices for both employees and non-employees were primarily due to officials issuing replacement devices for lost or damaged devices without deactivating old devices or regularly monitoring active devices. Timely deactivation of unneeded devices is an important component of access management and should coincide with the issuance of replacement devices. While a damaged and inoperable device may not be a risk for unauthorized access, a lost active device poses an increased risk for unauthorized access which officials should address through immediate deactivation.

Non-Employee Devices No Longer Needed –17 Schools (85 percent) had active individual non-employee accounts and devices that were no longer needed, and 18 Schools (90 percent) had shared devices that were no longer needed. Of the 5,134 non-employee accounts and devices we reviewed, 632 individual non-employee devices and 377 shared devices were no longer needed.

The individual non-employee devices that were no longer needed were associated with former employees, first responders no longer employed by the agency serving the School, and former vendors or contractors. The shared devices that were no longer needed included devices provided to substitute staff, first responders or vendors. However, in most of the selected Schools, these devices were not tracked or monitored, no one regularly reviewed them to determine whether access was still needed, and devices and were often missing without officials’ knowledge. Some devices were never used, while others were last used in 2020 and 2022.

System Reporting and Functionality – At all 20 Schools, officials used systems to manage building access that could generate reports showing last access activity, no activity or multiple access devices for individuals. However, at nearly every School these system-generated reports were often not part of regular monitoring of building access. Figure 2 is an example of the information that was readily available in one of the most common systems in use at the selected Schools, showing the name of the individual with access, the status of the access account as well as details about all devices issued to the individual. In this example, it is apparent that two individuals were issued multiple active devices. Had School officials used this system function, they could have readily identified and addressed the unneeded devices we identified in the audits.

Figure 2: System User Activity Report

Last Name	First Name	Middle Name	ID Status	Issue	Activate	Deactivate	Token #	Roles	Groups
			Active	03/26/2020			36286		
			Active	12/09/2024	12/09/2024	02/25/2034	37891		
			Active	09/14/2021	11/13/2025	01/30/2035	37945		
					09/14/2021	12/01/2030	37491		
					10/11/2023	12/27/2032	37826		
					05/15/2024	08/01/2033	37789		
			Active	03/26/2020	03/26/2020	12/31/2037	36997		
					03/26/2020	12/31/2037	36166		

Furthermore, though the Schools’ systems often had the function to automatically deactivate devices at a designated date, most officials did not use it. Figure 3 is an example of a system-generated report showing the last date that an active device was used and a specified date that a device was set to automatically deactivate.

Figure 3: System Device Activity Report

Name	Status	Embossed #	Internal #	Issue	Activate	Deactivate	Last Used
[REDACTED]	Active	36168	36168				09/19/2024 12:00:50
	Active	1175	1175				
	Active	36587	36587				06/10/2020 12:28:20
	Active	1197	1197				
	Active	36219	36219				
	Active	37308	37308				01/16/2026 08:34:00
	Active	37270	37270				01/20/2026 08:35:04
	Active	36439	36439				06/14/2024 15:24:05
	Active	36487	36487	03/26/2020 11:14:18	08/15/2022 10:03:31	12/31/2037 23:59:59	06/25/2021 08:12:25
	Active	36776	36776	03/26/2020 11:14:18	03/26/2020 11:14:18	12/31/2037 23:59:59	12/11/2025 07:14:38

Had School officials used this system function, they could have monitored and tracked the activity and use of their non-employee accounts and devices, limited access to defined periods of time and established deactivation of devices on specific dates.

Although similar reports were available in all Schools' systems, most of the 20 Schools we reviewed did not use them. Specifically:

- Only two Schools periodically generated reports and reviewed active accounts and devices.
- One School reviewed access activities only for one of their eight buildings.
- One School's review was limited to employees only.
- One School's review was limited to employees that left employment and non-employees' access after May 2024, when a form was implemented with expiration dates for access.

In addition, in one School where the system's function to automatically deactivate devices at a designated date was in place, officials were not aware that the function was applied to necessary devices for first responders. As a result, the first responders' necessary devices were deactivated. This was an oversight that officials could have avoided had they periodically reconciled and reviewed devices.

Periodic reconciliation and review of first responders' devices is particularly important, because reliable access devices are critical when life and safety depend on immediate response. However, none of the 20 Schools periodically scheduled or performed access attempt exercises to ensure all the first responders' devices were accounted for and functioned. When these devices have extended periods of inactivity, which was the case in most of the 20 Schools, officials should consider periodically verifying that these devices are accounted for and function as intended.

To aid officials in implementing impactful improvements, we reviewed system reports with officials and showed them how to incorporate these reports into their access monitoring. School officials are encouraged to use these reports in their monitoring and management operations for an efficient, timely identification and resolution of access concerns.

The Schools had inadequate, outdated or no building access account monitoring procedures.

None of the 20 Schools had adequate building access account monitoring procedures, and 12 Schools (60 percent) did not have any written policies and procedures outlining who is responsible for managing and monitoring accounts. Most school officials did not define who was authorized to create accounts or who was responsible for monitoring active accounts and devices. Policies and procedures also lacked guidance in revoking access (i.e., deactivating unneeded accounts and collecting devices).

While eight of the 20 Schools had written policies and procedures, they were either incomplete (e.g., limited to employee access only and did not contain provisions for non-employee accounts and devices, including shared devices), were outdated, or in some instances did not reflect existing practices and, therefore, were not always followed.

The process of adding access accounts was similar in all 20 Schools, and consisted of staff:

- Adding accounts for new employees to the system.
- Setting any access restrictions (e.g., time or a specific entry point) based on the employee's role and required access.
- Adding accounts for non-employees including shared devices, vendors and contractors.
- Printing and issuing devices to employees and non-employees.

In addition, only six Schools used written forms to document device issuance, such as device application forms. These forms included the name, position and other information relevant to building access. Although using written forms and maintaining adequate documentation can be a key part of the process that supports access management, some Schools used forms that were incomplete, lacked authorizing signatures, or did not specify access restrictions for the users. When documentation lacks important information, its usefulness for identifying potential access concerns is diminished. Furthermore, in Schools that did not use forms at all, officials had difficulty identifying individuals with access because there were no supporting forms or other documentation available to support why access was provided or who authorized it.

Seventeen of the 20 Schools (85 percent) used a manual process for adding user accounts to their systems. We observed that process of manual data entry led to errors in the systems:

- The process of adding users to the system often did not utilize a common identifier (e.g., employee identification number) between their Human Resources (HR) information system and the building access system.
- In Schools that used an individual's first and last name, we identified that naming differences between the systems (e.g. use of nicknames, misspellings or name changes) posed challenges in the reconciliation process.
- In Schools that relied on manual data entry and reconciliation, responsible employees often made changes in the system based on their review of their respective board's meeting minutes, information about staffing changes from other departments, or even their memory. As a result, updates to accounts were not always made in a timely manner, tracked or supported, leading to unnecessary active accounts and devices.

Conversely, we observed fewer issues in Schools using an automated process. Three Schools implemented an automated process for adding, modifying and revoking employee accounts utilizing Information Technology (IT) or HR software and building access system integration. Schools were most successful in managing access when they leveraged multiple information systems to periodically synchronize and share access changes. There were shared unique identifiers between systems, which made the account review process easier and more effective, because activating or deactivating a user in the HR or network access system automatically activated or deactivated the user's access in the building access system. Generally, these Schools had the most current access when we reviewed and compared access for employees and other individuals.

Best practices we observed

During our fieldwork at the Schools, we observed several practices that contributed to more effective building access management. Schools that were more effective often had processes or procedures that:

- Conducted a periodic review of the active accounts and communicated the results to the Superintendent or other responsible School officials.
- Deactivated all access at the end of the School year and then reactivated access at the start of the next School year based on updated employee rosters.
- Set automatic expiration dates or pre-determined lengths of access for non-employee access except access for first responders.
- Established communication between the system and the School's HR or network access software to automatically update employee access based on employee status changes, such as retirement or termination.
- Added first responder agency identification devices to the system, which in turn allowed those individuals access without the need for School-issued devices.

It is important to note that these processes or procedures alone do not guarantee effective access management. However, when multiple processes or procedures are implemented together and coupled with clearly assigned roles and responsibilities for staff involved in building access management processes, the School officials would likely improve their access management.

Conclusion

School officials are responsible for ensuring the safety of students, staff, and visitors while using School facilities. They should establish and follow policies that clearly assign responsibility for managing and monitoring building access, including entry protocols for all individuals.

Effective building access management is attainable with the Schools' current systems and with little to no additional resources. It often requires a better understanding of the systems in use and of the reports and settings available to officials for managing and monitoring building access. In some cases, improving access management is as simple as generating a report or adding a setting to existing access configurations.

Implementing scheduled periodic review of access utilizing available reports, immediately deactivating credentials for separated personnel, and establishing clear protocols for vendors' access devices can help close security gaps in these processes without requiring additional hardware or financial investments. By leveraging the system capabilities already available to officials, they can ensure a safer environment for students, staff and the broader educational community.

Appendix A: Background and Relevant Standards

According to the New York State Education Department (NYSED) data as of June 24, 2026, there are 730 school districts and 4,383 public schools⁵ and 37 BOCES⁶ in New York. The New York State legislature created BOCES to provide shared educational programs and services to school districts within the state. BOCES partner with school districts to provide a broad range of services that help meet the evolving educational needs of students.

School districts are governed by an elected board of education (board) charged with general control, while BOCES is governed by a board elected by the members of the component school districts' boards of education. Boards at the school districts and BOCES are responsible for managing and controlling the financial and educational affairs of these entities. A superintendent of a school district or BOCES' district superintendent is responsible, along with other administrative staff, for managing the entity's day-to-day operations under the board's direction.

NYSED's Safe Schools by Design Act guidance⁷ provides that, as the second line of defense when protecting a building and its occupants, building entry should maintain a welcoming exterior while ensuring safety and security, such as using credentialed electronic access systems. The Cybersecurity and Infrastructure Security Agency's (CISA) K-12 School Security Guide recommends schools should have in place a layered, system-based approach to physical security in which physical security equipment and technology, site and building features, personnel and staff, policies and procedures, and training programs work together to ensure school facilities are secure.

Policies and Procedures – Schools should develop and implement physical security and access control policies and procedures with roles and responsibilities defined and assigned across its organizational entities (e.g., IT, HR, administration, facilities, etc.). Policies and procedures should be established to manage, monitor and revoke building access devices and other access credentials as necessary. The policies and procedures should be periodically reviewed and updated to reflect the current and approved access controls implemented within the system and organization.

Building Access/Entry – Schools should control who can enter school buildings, where they can go, and when access is permitted. Building access systems serve as an internal control to help ensure safety and security including controlled entry points, visitor management and monitoring building access. Internal controls over building access/entry should be designed in a way that primary entrances are controlled through device readers, security desks or locked-door systems.

Building Access Account Management – Only designated system users/administrators should be able to create, enable, modify, revoke and remove accounts in accordance with documented policies and procedures. System administrators for access management should be limited and have clearly defined roles and responsibilities. Account management processes should align with individual status changes, such as extended leave, termination or other circumstances when access is not required.

Device Issuance and Authorization – Devices should only be issued with documented approval based on job role and building assignment; each device should be unique and individually assigned. Each individual should only have one device. Shared devices should be avoided so that all activity can be logged to a specific individual. When shared devices must be used, a process should be established to track these devices. No individual should be issued a device until a background check is completed, if required. Visitors and contractors should sign in at a single point of entry and receive a visible identification or badge. Contractors' access should be limited to approved locations and timeframes.

Device Management – Devices should be immediately deactivated when no longer necessary. Any necessary updates to building access should happen promptly. Lost or stolen devices should immediately be reported to staff responsible for deactivating devices and replacement devices should be reissued only with documentation approving the reissuance. Device inventory should be tracked, and periodically reconciled and unused or returned devices should be secured or destroyed.

Building Access Event Monitoring – Device events should be logged by user, door and timestamp (i.e., device used at door). These logs should be reviewed periodically and/or upon an unauthorized incident. The building access system should generate alerts for after-hours or unauthorized access attempts if possible. Logs should be retained according to the school's policies. Periodically reviewing physical access logs can help identify unexpected activity.

Additional Resources

We also used the following publications to inform our criteria. These publications provide school officials with actionable, practical and cost-effective resources, solutions and tools that enhance school building safety and security:

- **NYSED Safe Schools by Design Act: A Guide by NYSED (April 2025)**
<https://www.nysed.gov/sites/default/files/programs/facilities-planning/safeschoolsbydesign-aguidebynysed-april2025.pdf>
- **Partner Alliance for Safer Schools (PASS) Safety and Security Guidelines for K-12 Schools (7th Edition, 2025)**
https://passk12.org/wp-content/uploads/2025/08/PASS_7thEdition-web.pdf
- **K-12 School Security Guide (3rd Edition, 2022)**
<https://www.cisa.gov/sites/default/files/2022-11/k12-school-security-guide-3rd-edition-022022-508.pdf>
- **National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations (Revision 5)**
<https://www.cisa.gov/sites/default/files/2022-11/k12-school-security-guide-3rd-edition-022022-508.pdf>

In addition, local officials can use OSC's website to search for audits, resources, publications and training for officials at: <https://www.osc.ny.gov/local-government>

Appendix B: Selected Schools – Accounts and Devices Reviewed

Figure 4: Selected Schools – Accounts and Devices Reviewed

School	Active Devices	Current Employee Devices	Individual Non-Employee Devices	Shared Non-Employee Devices	Unneeded Devices Identified Number/ (Percentage)
Auburn City SD ^d	1,276	828	311	137	48 (4%)
Batavia City SD ^{cd}	792	594	68	130	94 (12%)
Brentwood UFSD ^a	2,839	2,644	187	8	8 (< 1%)
Broadalbin-Perth CSD ^c	477	395	26	56	17 (4%)
Central Square CSD ^c	947	798	104	45	28 (3%)
East Rochester UFSD ^{cd}	983	337	595	51	239 (24%)
Eldred CSD ^c	252	196	42	14	65 (26%)
Green Island UFSD ^b	114	67	28	19	12 (11%)
Greene CSD ^c	359	238	54	67	17 (5%)
Groton CSD ^c	179	159	12	8	10 (6%)
Holley CSD ^{cd}	423	254	90	79	73 (17%)
Malverne UFSD ^{cd}	420	351	45	24	44 (10%)
New York Mills UFSD ^b	117	74	41	2	1 (< 1%)
Niskayuna CSD ^d	1,209	997	127	85	67 (6%)
North Collins CSD ^{cd}	280	167	90	23	21 (8%)
Onondaga-Cortland-Madison BOCES ^c	1,308	846	192	251	228 (17%)
Orange-Ulster BOCES	1,535	1,407	107	21	138 (9%)
Red Hook CSD ^{cd}	827	457	353	17	94 (11%)
Union Endicott CSD ^d	1,688	742	499	447	181 (11%)
Waterloo CSD ^d	1,170	491	188	491	179 (15%)
Totals	17,195	12,042	3,159	1,975	1,564 (9%)

- a) Properly monitored and tracked shared devices.
- b) Did not have any employees with duplicate active devices.
- c) Did not have any written policies and procedures.
- d) Had non-employees with duplicate active devices.

Notes

1 Including 11 Central School Districts (CSD), five Union Free School Districts (UFSD), two City School Districts (City SD) and two BOCES. See Appendix B for a list of the Schools selected.

2 For this report, a first responder is any individual that may respond to an emergency at a school including, but not limited to, fire department personnel, emergency medical technicians, paramedics, local police, county sheriff deputies or New York State Police.

3 A shared account or device is assigned to a user for a specific role or function but not assigned to a specific individual.

4 The individual reports linked in Appendix B are also available at: <https://www.osc.ny.gov/local-government/audits>

5 <https://data.nysed.gov/>

6 <https://data.nysed.gov/lists.php?type=boces>

7 <https://www.cisa.gov/sites/default/files/2022-11/k12-school-security-guide-3rd-edition-022022-508.pdf>

Contacts



New York State Comptroller
THOMAS P. DINAPOLI

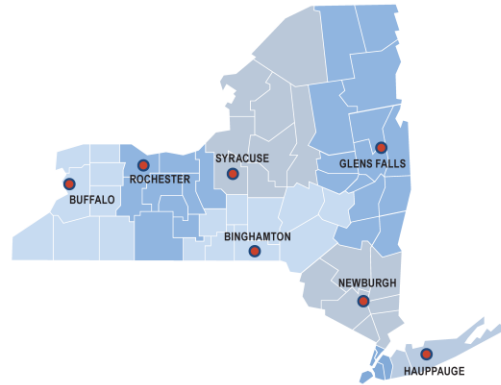
Division of Local Government and School Accountability

110 State Street, 12th Floor, Albany, NY 12236

Tel: 518.474.4037 • Fax: 518.486.6479

Email: localgov@osc.ny.gov

www.osc.ny.gov/local-government



Andrea C. Miller
Executive Deputy Comptroller

Executive • 518.474.4037
Robin L. Lois, CPA, Deputy Comptroller
Randy Partridge, Assistant Comptroller

**Audits, Local Government Services and
Professional Standards • 518.474.5404**
(Audits, Technical Assistance, Accounting and Audit Standards)

**Local Government and School Accountability
Help Line • 866.321.8503 or 518.408.4934**
(Electronic Filing, Financial Reporting, Justice Courts, Training)

Division of Legal Services
Municipal Law Section • 518.474.5586

**New York State & Local Retirement System
Retirement Information Services**
Inquiries on Employee Benefits and Programs
518.474.7736

Technical Assistance is available at any of our Regional Offices

BINGHAMTON REGIONAL OFFICE
Tel 607.721.8306 • Fax 607.721.8313 • Email Muni-Binghamton@osc.ny.gov
Counties: Broome, Chemung, Chenango, Cortland, Delaware, Otsego, Schoharie, Tioga, Tompkins

BUFFALO REGIONAL OFFICE
Tel 716.847.3647 • Fax 716.847.3643 • Email Muni-Bufferalo@osc.ny.gov
Counties: Allegany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming

GLENS FALLS REGIONAL OFFICE
Tel 518.793.0057 • Fax 518.793.5797 • Email Muni-GlensFalls@osc.ny.gov
Counties: Albany, Clinton, Columbia, Essex, Franklin, Fulton, Greene, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Warren, Washington

HAUPPAUGE REGIONAL OFFICE
Tel 631.952.6534 • Fax 631.952.6530 • Email Muni-Hauppauge@osc.ny.gov
Counties: Nassau, Suffolk

NEWBURGH REGIONAL OFFICE
Tel 845.567.0858 • Fax 845.567.0080 • Email Muni-Newburgh@osc.ny.gov
Counties: Dutchess, Orange, Putnam, Rockland, Sullivan, Ulster, Westchester

ROCHESTER REGIONAL OFFICE
Tel 585.454.2460 • Fax 585.454.3545 • Email Muni-Rochester@osc.ny.gov
Counties: Cayuga, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates

SYRACUSE REGIONAL OFFICE
Tel 315.428.4192 • Fax 315.426.2119 • Email Muni-Syracuse@osc.ny.gov
Counties: Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego, St. Lawrence

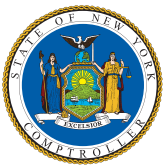
STATEWIDE AUDIT
Tel 716.847.3647 • Fax 716.847.3643 • Email Muni-Statewide@osc.ny.gov

APPLIED TECHNOLOGY UNIT
Tel 518.738.2639 • Fax 518.486.6479 • Email Muni-Cyber@osc.ny.gov

osc.ny.gov



FOLLOW US: osc.ny.gov/subscribe



Contact

Office of the New York State Comptroller
110 State Street
Albany, New York 12236
(518) 474-4044

<https://www.osc.ny.gov>

Prepared by the Division of Local Government and School Accountability
Statewide Audits Unit

 FOLLOW US: [osc.ny.gov/subscribe](https://www.osc.ny.gov/subscribe)