

New York State Comptroller
THOMAS P. DiNAPOLI

North Collins Central School District

Building Access

July 2026 | S9-26-16

Prepared by the Division of Local Government and School Accountability

Table of Contents

Audit Results	1
Building Access: Finding and Recommendations	3
Finding 1 – District officials did not properly manage and monitor building access accounts and badges.	3
Recommendations	4
Appendix A: Profile, Criteria and Resources	5
Profile	5
Criteria	5
Additional Resources	6
Appendix B: Response From District Officials	7
Appendix C: Audit Methodology and Standards	8

Audit Results

North Collins Central School District

Audit Objective

Did North Collins Central School District (District) officials properly manage and monitor building access accounts and devices?

Audit Period

July 1, 2024 – November 30, 2025

We extended our audit period to February 3, 2026 to review access activity logs.

Understanding the Audit Area

Building access controls are essential for enhancing security and enabling school officials to manage and monitor entry points within educational institutions. These systems authenticate a 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 in this way, schools can better safeguard their facilities and maintain a safe and secure environment for students, teachers, staff and visitors.

The District uses a building access management system (system) which included 280 active building access accounts (accounts) associated with 167 devices issued to current employees, and 113 issued to non-employees including 23 shared devices.¹ Each of the District's two school buildings have one public point of entry. Employees can also use other points of entry, which require a device to enter the building.

Audit Summary

District officials did not properly manage and monitor building access accounts and devices (badges). As a result, there was a potential risk for unauthorized access to District school buildings, compromising building security and safety for students, teachers, staff and visitors. Specifically, of the accounts we reviewed, the District had 17 active, but unneeded, non-employee accounts with assigned badges in the system, including:

- 11 badges issued to individual non-employees, and
- Six shared badges.

Although District officials had a process for adding accounts in the system for employees and non-employees, there was no process for promptly disabling or deleting accounts when no longer needed. Furthermore, these issues occurred because no one periodically reviewed active accounts to determine whether they were needed.

This report includes three recommendations that, if implemented, will help District officials improve management and monitoring of building access accounts and badges. District officials generally agreed with our recommendations and their response is included in Appendix B.

¹ A shared account or device is assigned to a user for a specific role or function but not assigned to a specific individual (e.g., vendors or first responders).

This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the Office of the New York State Comptroller's (OSC's) authority as set forth in Article 3 of the New York State General Municipal Law (GML). The audit's methodology and standards are included in Appendix C.

The Board of Education (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 OSC within 90 days, pursuant to Section 35 of GML, Section 2116-a (3)(c) of the 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 the CAP, please refer to the OSC brochure, *Responding to an OSC Audit Report*, which was provided with the draft audit report. The CAP should be posted on the District's website for public review.

Building Access: Finding and Recommendations

Properly managing and monitoring building access is a fundamental security function and the responsibility of school district officials. Various resources, publications, and guides are available to help school district and Board of Cooperative Educational Services (BOCES) (together, “schools”) officials develop and implement necessary building access infrastructure and systems to create a safe and secure environment for their students, teachers, staff and visitors.

More details on the criteria used in this report, as well as resources OSC makes available to local officials that can help them improve operations, are included in Appendix A.

Finding 1 – District officials did not properly manage and monitor building access accounts and badges.

During our fieldwork in February 2026, the District had 280 active accounts associated with 167 badges issued to current employees, and 113 badges issued to 90 individual non-employees including 23 shared badges. We determined:

- 12 percent of active individual non-employee accounts and badges were unneeded, and
- 26 percent of active shared accounts and badges were unneeded.

Non-Employee Accounts – Of the 90 individual non-employee accounts, 79 were assigned to individuals who had legitimate business needs to access District school buildings, such as BOCES employees and service providers. However, the remaining 11 accounts and badges (12 percent) were not needed and District officials should have deactivated them:

- Eight badges were assigned to former employees who separated from District employment including two badges that were unused since activation,
- Two badges were assigned to third-party vendors that were no longer under contract with the District, and
- One badge was assigned to a retired BOCES employee who previously provided services to the District.

The Superintendent told us that the District implemented a process in June 2025 to deactivate all accounts and badges for employees at the end of each school year, then re-activate the accounts for active employees shortly before the new school year begins. However, this process was not operating effectively, because we found eight active accounts and badges for former employees. For example, we identified a former employee who separated from District employment in January 2023 with an active account and badge. If this process was functioning as intended, no former employees would have active accounts and badges that would provide access to District buildings.

Additionally, the District Clerk stated that, also as of June 2025, District officials and employees started using a checklist for employees separating from the District that includes an action item for the technology department to deactivate the departing employees’ accounts. Prior to using this checklist, the District Clerk told us she requested that the technology department deactivate separating employees’ accounts either via email or in person. Furthermore, the Director of Technology (Director) stated that his department did not receive requests to deactivate unneeded accounts as evidenced by the three accounts that remained active for contracted vendors and a retired BOCES employee. Prompt deactivation of building access when it is no longer needed is an important component of access management and decreases the risk of unauthorized access.

When we brought these issues to District officials' attention, the Director deactivated the accounts and badges, which we observed. However, District officials should have deactivated the accounts as soon as they were no longer needed, such as when a vendor's contract or an individual's employment with the District ended. Because the District did not have adequate procedures to routinely review and deactivate badge accounts, these accounts remained active and could potentially have been used for unauthorized access.

The 23 active shared badges included 17 that were necessary and for District purposes, including first responders, substitute employees and student teachers. However, we determined the remaining six shared badges were no longer needed and should have been deactivated:

- Four badges were assigned to contractors who were involved with the District's 2022 capital project,
- One badge was assigned to a parent-teacher association president, and
- One account and badge that District officials could not explain why it was created.

Because the District did not have a clear communication of responsibilities or documented procedures for managing and monitoring building access, there remains a risk that access devices are not collected. Also, there was no reconciliation of accounts and badges, which increased the risk of unauthorized entry.

Account Management and Monitoring Procedures – Although the District Clerk maintained checklists to add, modify and revoke badge accounts for District employees, District officials did not have any written procedures outlining roles and responsibilities for managing and monitoring badge accounts. Specifically, District officials did not define who is authorized to create accounts, who is responsible for monitoring active accounts, and the process to revoke access, by deactivating unneeded accounts and collecting badges.

At the time of our fieldwork, requests to add, modify or revoke badge accounts for District employees were initiated by the District Clerk and communicated to the technology department. Similarly, requests for shared badge accounts, such as those used by substitute employees and contracted vendors, were initiated by the responsible department heads and communicated to the technology department. Technology department employees made the requested additions or modifications in the system. However, there were no written procedures or documentation outlining how these accounts should be managed and monitored. As a result, account updates were not always made in a timely manner and there was a potential for unauthorized access to District buildings due to untimely account deactivation.

Recommendations

District officials should:

1. Deactivate accounts and collect the associated badges as soon as they are no longer needed.
2. Develop written procedures that define who is responsible for managing and monitoring accounts including shared badges and periodically evaluate and adjust these procedures to ensure all processes are working as intended.
3. Develop a reconciliation process utilizing system reports, and review active accounts for necessity and appropriateness of access.

Appendix A: Profile, Criteria and Resources

Profile

The District serves the Towns of Brant, Collins, Concord, Eden, Evans and North Collins in Erie County. The District's buildings are located on campuses in the Town of North Collins.

The District is governed by the elected seven-member Board. The Board is responsible for managing and controlling the District's financial and educational affairs. The Superintendent is responsible, along with other administrative staff, for managing the District's day-to-day operations under the Board's direction.

The District Clerk is responsible for initiating requests to add, modify and revoke employee accounts and their associated badges. Department heads are responsible for initiating requests to add, modify and revoke non-employee accounts and their associated badges. The Director² and technology department staff are responsible for managing and monitoring accounts by utilizing the system and printing and issuing badges to individuals which are then distributed either by the technology department or other department heads.

Criteria

NYSED's Safe Schools by Design Act guidance³ 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 Guide⁴ 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, Human Resources (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

² The Director was hired in September 2025.

³ <https://www.nysed.gov/sites/default/files/programs/facilities-planning/safeschoolsbydesign-aguidebynysed-april2025.pdf>

⁴ <https://www.cisa.gov/sites/default/files/2022-11/k12-school-security-guide-3rd-edition-022022-508.pdf>

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 district 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://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.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: Response From District Officials

The content below is a reproduced copy of the original response letter issued by District officials, is reformatted to meet the Americans with Disabilities Act *Web Content Accessibility Guidelines (WCAG)*,⁵ and may have included changes to spelling and grammar. The substance of the content was not changed.

NORTH COLLINS CENTRAL SCHOOL DISTRICT
P.O. Box 740
North Collins, NY 14111

July 23, 2026

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

Subject: Official Response to Draft Audit Report - Building Access Accounts and Devices
(Audit Period: July 1, 2024- November 30, 2025)

To the Office of the New York State Comptroller:

The North Collins Central School District (the "District") is in receipt of the draft audit report prepared by your office concerning the management and monitoring of our building access accounts and devices for the period of July 1, 2024, through November 30, 2025, with extensions through February 3, 2026. On behalf of the Board of Education and the District Administration, we appreciate the professional insight and thoroughness demonstrated by your field audit team.

Ensuring a safe, secure, and welcoming environment for our students, teachers, staff, and visitors remains the highest priority of the district. We recognize that robust internal controls over electronic building access systems are fundamental to maintaining our facility security.

The district does not dispute the findings in the report. We are in the process of preparing a Corrective Action Plan, which will take into consideration the audit recommendations. Once finalized, the plan will be posted to the district's website for public review. We thank your office for assisting the district in strengthening our administrative safeguards to better protect our school community.

Sincerely,

Scott J. Taylor
Superintendent

⁵ <https://www.ada.gov/resources/2024-03-08-web-rule/#highlights-of-the-requirements-in-the-rule>

Appendix C: Audit Methodology and Standards

OSC auditors obtained an understanding of internal controls that were deemed significant within the context of the audit objective and assessed those controls. Information related to the scope of the work on internal controls, as well as the work performed in the audit procedures to achieve the audit objective and obtain valid audit evidence, included the following:

- We interviewed District officials and reviewed Board policies to gain an understanding of the District's policies, procedures and practices related to managing and monitoring building access accounts and badges, including roles and responsibilities of the individuals involved in the process.
- We compared the District's 280 active building access accounts list to the employee master list of 167 employees to determine whether all accounts were associated with current District employees. We interviewed District officials and reviewed relevant documentation to determine whether the building access accounts and badges assigned to non-employee users were necessary. For any unnecessary accounts, we inquired as to why they were not deactivated.
- We used our professional judgment to select 11 of the 17 necessary accounts for shared badges and all six unneeded accounts for shared badges and inquired with the respective District officials responsible for these badges to determine whether they were in their possession. If the badges were not in their possession, we inquired to determine why and attempted to locate the badges.

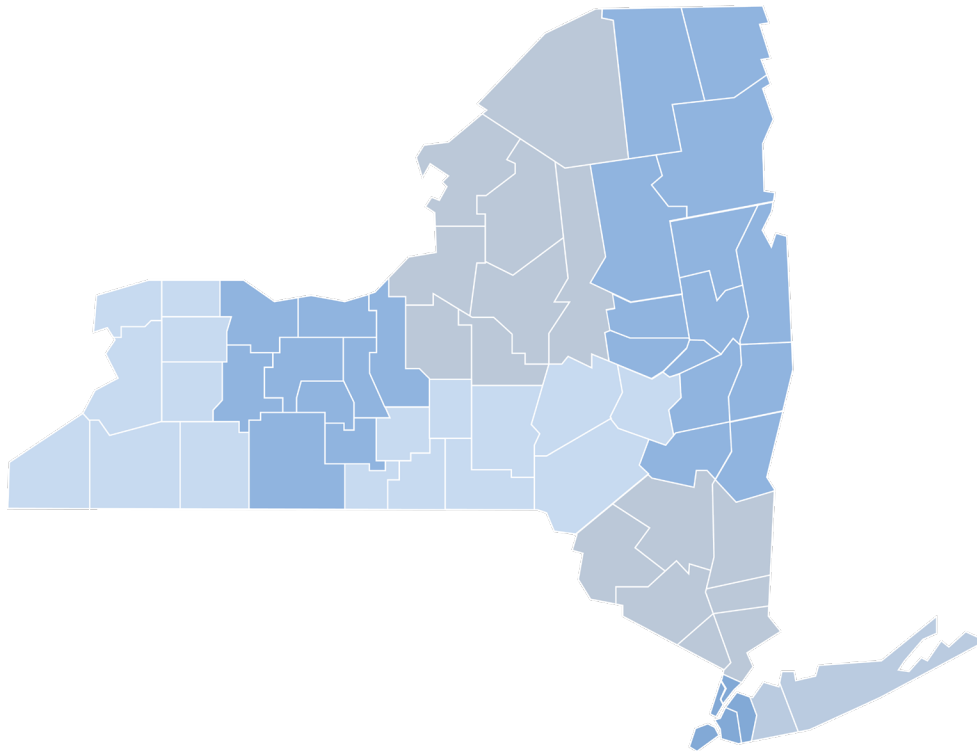
OSC auditors conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that auditors plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on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

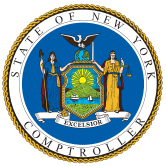
Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or relevant population size and the sample selected for examination.

Questions?

STATEWIDE AUDITS

Nicole A. Tomsen, Chief of Municipal Audits
295 Main Street, Suite 1032 • Buffalo, New York 14203-2510
Tel (716) 847-3647 • Fax (716) 847-3643
Email: Muni-Statewide@osc.ny.gov





Contact

Office of the New York State Comptroller
110 State Street
Albany, New York 12236

(518) 474-4044

www.osc.ny.gov

Prepared by the Division of Local Government and School Accountability



FOLLOW US: osc.ny.gov/subscribe