

New York State Comptroller
THOMAS P. DiNAPOLI

Waterloo Central School District

Building Access

August 2026 | S9-26-8

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	9

Audit Results

Waterloo Central School District

Audit Objective

Did Waterloo 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 April 20, 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 utilizes a building access management system (system) with 1,170 active building access accounts (accounts), including 491 devices issued to current employees and 679 issued to non-employees, of which 491 are shared devices.¹ The District's five buildings each have a single public point of entry. Employees may also access the buildings through additional secured entry points, which require a device for entry.

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 the District school buildings, compromising building security and safety for students, teachers, staff and visitors. Specifically, of the accounts we reviewed, the District had active, but unneeded, accounts with assigned badges in the system:

- 106 individuals, including 86 employees and 20 non-employees, had two or more active badges, including eight employees and two non-employees with three or more active badges.
- 56 badges (8 percent) of 679 non-employee accounts were unneeded.
- District officials could not locate 37 out of 78 (47 percent) requested badges.

Although District officials had a written procedure for adding accounts in the system for employees and non-employees, no one regularly monitored or reviewed active accounts to determine whether they were needed. Furthermore, these issues occurred because District officials did not develop written policies and procedures that clearly assign roles and define the responsibilities for managing and monitoring accounts or issuing badges.

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 report includes four 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.

This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of 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 we make 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 April 2026, the District had 1,170 active accounts associated with 491 badges issued to 390 employees and 679 badges issued to non-employees,² including 491 shared badges. We determined:

- 86 employees (22 percent) and 20 non-employees (3 percent) had two or more active badges, and
- 56 non-employee badges (8 percent) were unneeded.

Employee Accounts – Of the 390 current employees, 86 employees (22 percent) were assigned two or more active badges, including eight employees who were each assigned three or more active badges.

We requested to observe badges of the eight employees that had three or more active badges, totaling 31 badges. District officials were unable to locate 12 of the 31 badges. The Network Analyst, who was assigned to manage and monitor accounts, explained that it was the District’s practice to issue two badges to employees in certain positions (e.g., custodians, administrators) as a matter of convenience, including these eight employees. The Network Analyst further explained that these eight employees lost one of their badges and were issued replacements, but it was also the District’s practice to leave the lost badges active in case they were found. However, each individual should only have one badge and District officials should deactivate lost badges as soon as possible; issuing duplicate badges for convenience and leaving lost badges active increases the risk of unauthorized access to school buildings. Importantly, officials did not have a procedure to periodically review active badges and determine whether duplicate or replacement badges remained necessary.

Although the Network Analyst ran a daily events report and reviewed it for suspicious activity, District officials did not use other available system reports, including reports showing badge activity and last-use dates, to periodically identify inactive or unnecessary badges.

Non-Employee Accounts – Of the 679 non-employee badges, we determined 56 active badges (8 percent) were unneeded. Of the 56 unneeded non-employee badges:

- 33 were shared badges with little to no activity: 20 badges were not used in at least six months and 13 were never used.
- 23 were assigned to individual non-employees, including 17 former vendors, four former employees and two community members to use school facilities. Nine of these badges were never used.

The Network Analyst told us District officials should have deactivated these accounts and collected the associated badges once they were no longer needed. However, the District did not have a formal process in place to ensure non-employee badges were necessary, including periodically reviewing system reports

² 310 shared badges only provide restricted access to a single interior classroom door or the bus gate. These badges do not open exterior doors.

detailing device access activity. As a result, these accounts and associated badges remained active and there was an increased risk of unauthorized access to District buildings. The Network Analyst told us that he planned to implement a procedure to deactivate all non-employee accounts after 30 days of inactivity.

In addition, 20 individual non-employees were issued two or more badges, including two individuals with three active badges. We requested to observe the badges of the two individual non-employees who each had three active badges, totaling six badges. District officials were unable to locate three of these badges. When we brought these issues with non-employee badges to District officials' attention, the Network Analyst promptly reviewed all active accounts and deactivated all unneeded individual, shared and duplicate badges.

These issues occurred, in part, due to a lack of clear responsibilities and documented procedures for managing and monitoring building access, including regularly reviewing system-generated access reports, reconciling active accounts to current authorized users and promptly deactivating accounts when access was no longer needed.

Account Management and Monitoring Procedures – District officials had written procedures for issuing, changing, and deactivating employee badges, but none for monitoring or deactivating badges for non-employees. The procedures did not require regular reviews of active accounts and badges to verify if access remained appropriate, nor did they assign responsibility for monitoring active accounts, reviewing shared badges, or regularly reconciling active access to supporting records.

At the time of our fieldwork, the Network Analyst and a Computer Support Specialist accessed the system to create, modify and deactivate badge access. The Network Analyst told us that access requests were initiated by the Human Resources (HR) department or District administrators and communicated by email. Although the Network Analyst reviewed the daily system activity report for unusual building entry activity, there was no periodic reconciliation of active accounts and badges to current employee and non-employee access lists to determine whether all active access remained appropriate. While a daily review of unusual activity is an important part of access management, integrating additional system reports, such as periods of inactivity and the last date of access, would improve monitoring and management of building access. This review process would help ensure that necessary access updates are made in a timely manner and, in turn, decrease the potential for unauthorized access to District buildings.

Recommendations

District officials should:

1. Consider discontinuing the practice of issuing multiple devices to employees.
2. Deactivate accounts and collect the associated badges as soon as they are no longer needed.
3. 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.
4. 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's boundaries include parts of the Towns of Fayette, Junius, Seneca Falls, Tyre and Waterloo in Seneca County. The District's school buildings are located in the Towns of Waterloo and Fayette.

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 Superintendent assigned the Network Analyst the responsibility for managing and monitoring accounts. The Network Analyst and Computer Support Specialist had administrative rights and full access to the system to print badges and activate, modify and deactivate user access accounts. Badges were distributed to individuals directly or to administrators (e.g., building principals).

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 their 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

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>

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 our 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 and 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.

District officials submitted their CAP along with their response. We did not include this information in the final report, as the response included sufficient information to indicate their intentions.

Waterloo Central School District
109 Washington Street, Waterloo, NY 13165
www.waterloocsd.org

Waterloo Central School District Response to Building Access Audit Division of Local Government and School Accountability Report S9-26-8

Waterloo Central School District (WCSD) appreciates the opportunity to review the findings contained in the Building Access Audit Report S9-26-8. The District acknowledges the importance of maintaining strong controls over building access accounts, badges, and devices to ensure the safety and security of students, staff, and facilities.

WCSD agrees that improvements are needed in the management and monitoring of building access accounts and devices. The District has reviewed the audit findings and has begun implementing corrective actions where appropriate.

Audit Finding 1

106 individuals, including 86 employees and 20 non-employees, had two or more active badges, including eight employees and two non-employees with three or more active badges.

District Response:

WCSD partially agrees with this finding. While the audit accurately identified individuals with multiple active credentials, the District believes there are operational circumstances that justify the issuance of more than one access credential to certain personnel.

Some employee job classifications require both an identification badge and a key fob for safety, security, and operational purposes. Additionally, identification badges are subject to normal wear and damage due to daily use, particularly in positions where badges are frequently handled or exposed to conditions that can cause them to break or become unusable. In these situations, replacement badges may be issued to ensure uninterrupted access and identification capabilities. The District recognizes, however, the need for stronger oversight to ensure that duplicate or replacement credentials are properly documented, monitored, and deactivated when no longer needed.

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

Audit Finding 2

56 badges (8 percent) of 679 non-employee accounts were unneeded.

District Response:

WCSD agrees with this finding. Following the audit review, the identified unnecessary credentials have been disabled. The District is also reviewing its procedures for managing non-employee access to ensure that access privileges are periodically reviewed and removed when no longer required.

Audit Finding 3

District officials could not locate 37 of the 78 (47 percent) requested badges.

District Response:

WCSD agrees with this finding. The badges that could not be accounted for have been disabled to eliminate any potential security risk. The District is evaluating and strengthening its badge inventory and tracking procedures to improve accountability for issued credentials and to ensure timely recovery of badges when individuals separate from service or no longer require access.

Additional Clarification Regarding Non-Employee Badges/Devices

In addition, the District maintains more than 100 access credentials for first responders, including members of local Fire Departments, Emergency Medical Services (EMS), and law enforcement agencies. These credentials are issued to support emergency response activities and facilitate rapid access to District facilities when needed to protect the safety and welfare of students, staff, and visitors. While WCSD acknowledges the audit's findings regarding the need for improved management and oversight of non-employee credentials, the District believes it is important to recognize the unique operational and public safety requirements associated with these categories of access devices. The District will continue to review all non-employee credentials periodically to ensure they remain authorized, appropriately assigned, and consistent with operational and emergency response needs.

Conclusion

Waterloo Central School District is committed to strengthening its building access controls and improving administrative oversight of access credentials. The District has taken immediate action to disable unnecessary or unaccounted-for badges and will continue to evaluate and enhance its procedures to ensure the proper issuance, monitoring, and recovery of building access devices.

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 access accounts and badges, including roles and responsibilities of the individuals involved in the process.
- We compared the District's 1,170 active building access accounts list to the employee master list to determine whether all accounts were associated with current District employees. We also compared the access accounts list to reports of current officers provided by local law enforcement. We interviewed District officials and reviewed relevant documentation, including the date the badges were last used, to determine whether active access accounts, shared badges and badges assigned to individual non-employee users were necessary. For any unnecessary accounts, we inquired as to why they were not deactivated.
- We used our professional judgment and selected 11 needed and nine unneeded badges (20 total) out of 188 non-employee badges based on user category and last access date and inquired with the 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.
- We used our professional judgment and selected 21 out of 181 shared accounts with exterior door access based on user category and last access date and inquired with the 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.
- We reviewed the active access accounts list to determine whether any users had more than one account and badge and interviewed District officials to determine why. We identified 106 individuals (86 employees, 20 non-employees) with a total of 123 duplicate badges (101 employees, 22 non-employees). We discussed these duplicate badges with District officials to determine why individuals had multiple badges. We then used our professional judgment to select eight employees with three or more duplicate badges, totaling 31 badges, and two non-employees with three or more duplicate badges totaling six badges and followed up with District officials to observe all badges sampled.

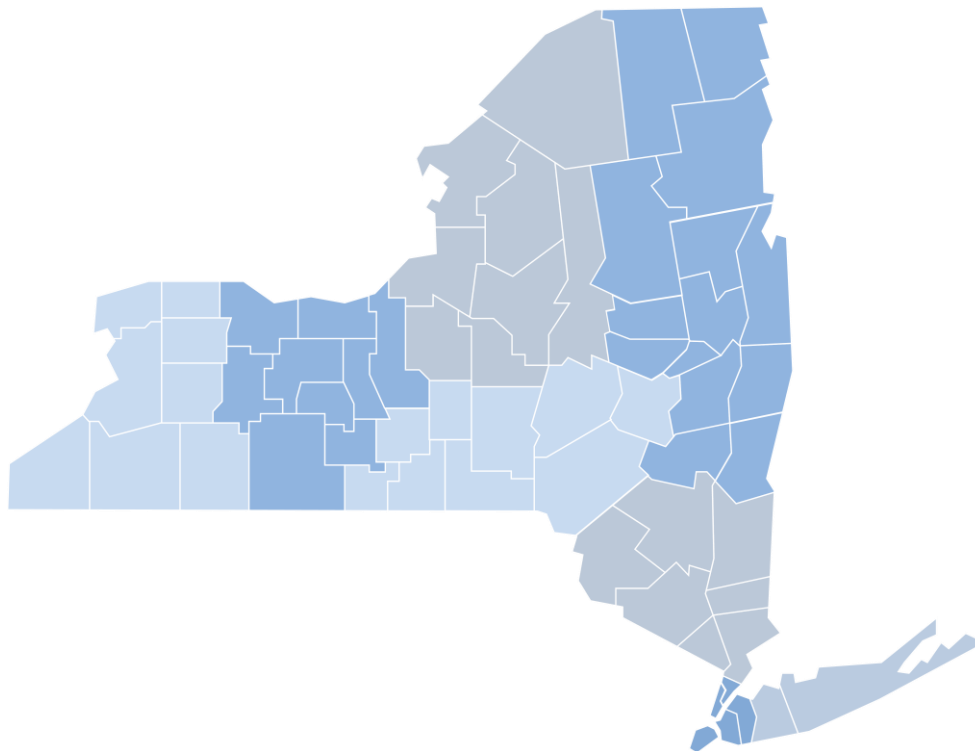
OSC auditors conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that auditors plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on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