

New York State Comptroller
THOMAS P. DiNAPOLI

Union-Endicott Central School District

Building Access

August 2026 | S9-26-9

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

Union-Endicott Central School District

Audit Objective

Did Union-Endicott 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 21, 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 1,675 active building access accounts (accounts) associated with 742 devices issued to current employees and 946 issued to non-employees including 447 shared devices.¹ Each of the District's seven school buildings has one 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 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:

- 11 individuals had two or more badges, including five employees who were assigned two active badges, five non-employees who were assigned two active badges and one non-employee who was assigned three active badges.
- 19 individual non-employee badges were not deactivated when building access was no longer needed.
- 150 shared badges, including 35 badges for substitute teachers which officials could not locate, were no longer needed but remained active. This occurred because the monitoring process for these shared badges was inconsistent and because District officials did not review the necessity of shared badges until our audit inquiry.

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).

Although District officials had a process for adding accounts in the system for employees and non-employees, no one periodically 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.

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 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 D.

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 building access management and monitoring 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 April 2026, the District had 1,675 active accounts associated with 742 badges issued to 737 current employees, and 946 badges issued to non-employees, including 447 shared badges. We determined:

- 11 individuals had unneeded duplicate active badges,
- 54 percent of individual non-employee accounts we reviewed were unneeded, and
- 34 percent of shared badges were unneeded.

Employee Accounts – Of the 737 employees, five employees were each assigned two active badges. We reviewed all five accounts associated with the badges with District officials and determined that one duplicate badge was created for the convenience of the employee, and the remaining four badges were issued as replacements for lost or damaged badges that District officials did not deactivate. After we brought it to District officials’ attention, the Director of Facilities and Safety (Director) deactivated all duplicate badges.

Non-Employee Accounts – For the individual non-employee accounts, we sampled and reviewed 35 of the 499 badges with District officials,² and determined that 19 of the 35 badges (54 percent) were no longer needed. Specifically:

- 10 badges were issued to former contractors that no longer provided services to the District.
- Eight badges were assigned to former District employees.
- One badge was assigned to an individual that the Director did not recognize.

In addition, we identified that six individual non-employees were assigned a total of 13 active badges, including five individuals with two active badges and one with three active badges. The Director told us that the duplicate badges were issued to three BOCES employees who provided services to the District, two employees of the District’s contracted badge system company and a contracted school psychologist. As with the duplicate employee badges, the Director told us badges were issued as replacement badges for lost or damaged badges that District officials did not deactivate. After we brought it to District officials’ attention, the Director deactivated the 19 badges that were no longer needed and the seven duplicate badges.

The 447 active shared badges included 233 substitute teacher badges. The Director told us that the main office secretaries for each school building had custody of these badges when they were not in use. We reviewed the process for tracking the substitute teacher badges and attempted to locate them at two buildings,

² See Appendix C for details of our sampling and testing methodology.

including 98 badges at one elementary school and 24 badges at the high school. We identified that the processes varied by building. Specifically:

- The elementary school did not have a process to require any sign-in sheet or maintain other documentation to verify which substitute teachers were assigned badges when distributing the 98 shared badges assigned to the elementary school. Although we verified that 63 of the 98 badges were accounted for and that they were stored in a secure location when not in use, District officials could not locate the remaining 35 badges.
- The high school main office secretary utilized a sign-in sheet to track the substitute teachers by name, along with the badge number they were assigned for the day, when distributing the 24 shared badges allotted to substitute teachers at the high school. The high school secretary had custody of all 24 badges.

After our audit inquiry, the Director told us that his department was adopting the high school's shared badge monitoring and tracking processes and planned to apply that process to all other District school buildings. The Director also told us that although all 447 shared badges were needed in the past, many of them were no longer needed. During our fieldwork, he reviewed all 447 shared badges and deactivated 150 badges (34 percent) as they were no longer needed, including the 35 badges that officials could not locate at the elementary school.

Account Management and Monitoring Procedures – Although District officials established a written procedure for adding, modifying and revoking access for employees, they did not have any written procedures that defined the process for adding, changing and deactivating accounts and devices for non-employees. At the time of our audit in May 2026, the Director's secretary (Secretary) was responsible for:

- Adding accounts for new employees to the system including 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 such as contractors, police and BOCES employees.
- Issuing prenumbered badges to employees and non-employees, and
- Collecting and deactivating badges that were no longer needed due to resignation, retirement or termination.

However, no one was periodically reviewing active accounts and badges to determine whether all active accounts and badges were needed. As a result, account updates were not always made in a timely manner and there was a potential for unauthorized access to District school buildings due to untimely account deactivation and duplicate badge deactivation. During our fieldwork, District officials began to update District policies and forms detailing procedures for non-employee badge access and monitoring accounts.

Recommendations

District officials should:

1. Ensure individuals do not have duplicate badges.
2. Deactivate accounts and collect the associated badges as soon as they are no longer needed.
3. Monitor the non-employee badges and shared badges at all schools to ensure they are accounted for and needed and deactivated if unaccounted for or unneeded.
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 the Town of Union in Broome County and parts of the Town of Owego in Tioga County. The District's seven school buildings are located on campuses in the Town of Union.

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 Director the responsibility for managing and monitoring accounts. The Secretary handles most of the building access and utilizes the system to print and issue badges which she distributes to individuals. The Director and a Personnel department staff member also have administrative rights to activate, modify and deactivate accounts in the system if the Secretary is unavailable to do so.

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.

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>

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 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.

Union-Endicott Central School District
1100 East Main Street
Endicott, New York 13760-5298
Telephone (607) 757-2103 Fax (607) 757-2809

August 10, 2026

Office of the State Comptroller
Binghamton Regional Office
44 Hawley Street
Binghamton, NY 13901-4417

Dear Audit Team:

The Union-Endicott Central School District is in receipt of the Draft Audit Report resulting from the audit of the District's Building Access Accounts and Badges for the period July 1, 2024, through April 21, 2026. Please accept this letter as the District's formal response to the findings and recommendations contained in the report.

The district appreciates the time and attention provided by the audit team throughout the review process, and in particular, the opportunity to discuss the findings and recommendations during the exit meeting. The District recognizes the importance of maintaining effective controls over building access accounts and badges and has already taken corrective action to address the matters identified during the audit.

FINDING: District officials did not properly manage and monitor building access accounts and badges.

RECOMMENDATIONS AND CORRECTIVE ACTIONS:

1. Ensure individuals do not have duplicate badges.

During the audit, duplicate badges were identified, deactivated, and removed from the access control system. The District will continue to monitor active badges to prevent duplicate access credentials from remaining active.

2. Deactivate accounts and collect the associated badges as soon as they are no longer needed.

The District has reinforced procedures for the timely deactivation of building access accounts and the collection of associated badges when access is no longer required. Going forward, District officials will periodically generate and review reports of active access accounts and badges to verify access remains necessary and appropriately assigned. Any account or badge determined to be no longer necessary will be deactivated and, when applicable, the associated badge will be collected.

3. Monitor the non-employee badges and shared badges at all schools to ensure they are accounted for and needed, and deactivated if unaccounted for or unneeded.

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

The District has strengthened its procedures for non-employee badges, including badges issued to BOCES staff and contractors. These requirements have been incorporated into Board Policy, Regulation, and Form 6118, *Identification Badges*. The District will continue to monitor non-employee and shared badges to ensure they are appropriately assigned, accounted for, and deactivated when access is no longer necessary.

The District remains committed to maintaining a comprehensive, layered approach to school safety and security. Existing security measures include School Resource Officers in all buildings, staff and secondary student identification badges, secure vestibule entry systems, security cameras, and artificial intelligence-based weapons detection systems at building entrances. The District views effective management of building access accounts and badges as an important component of this broader security framework. The corrective actions identified above have been implemented, and the District will continue these practices as part of its ongoing internal control procedures.

We appreciate the guidance provided by the audit team and believe the enhancements implemented as a result of this review will further strengthen our building security, improve accountability for building access, and help ensure the safest possible environment for our school community.

Thank you again for your collaboration and valuable feedback provided throughout the audit process.

Sincerely,

Nicole Wolfe, Ed.D.

Superintendent of Schools
Union-Endicott Central School District

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 our work on internal controls, as well as the work performed in our 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 accounts and badges, including roles and responsibilities of the individuals involved in the process.
- We compared the District's 1,675 active badge access accounts list to the employee master list to determine whether accounts existed that were not associated with current District employees. We interviewed District officials and reviewed relevant documentation to determine whether the accounts and badges assigned to non-employees were necessary. For any unnecessary accounts, we inquired as to why they were not deactivated.
- We used our professional judgment to select two of the seven schools that were allocated a total of 122 shared substitute employee badges to review that badges were accounted for. We selected the high school with 24 badges, and an elementary school with 98 badges, which was the highest number of shared badges for substitute employees among all schools. We 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. Additionally, we discussed all other shared badges with the Director and reviewed relevant documentation to determine if they were needed and how they were managed.
- We reviewed the active badge access accounts list to determine whether any individuals had more than one account and badge and interviewed District officials to determine why individuals were assigned more than one account. We identified 12 individuals with a total of 25 badges (five employees and seven non-employees). We followed up with the Director to determine why these individuals were assigned more than one badge.

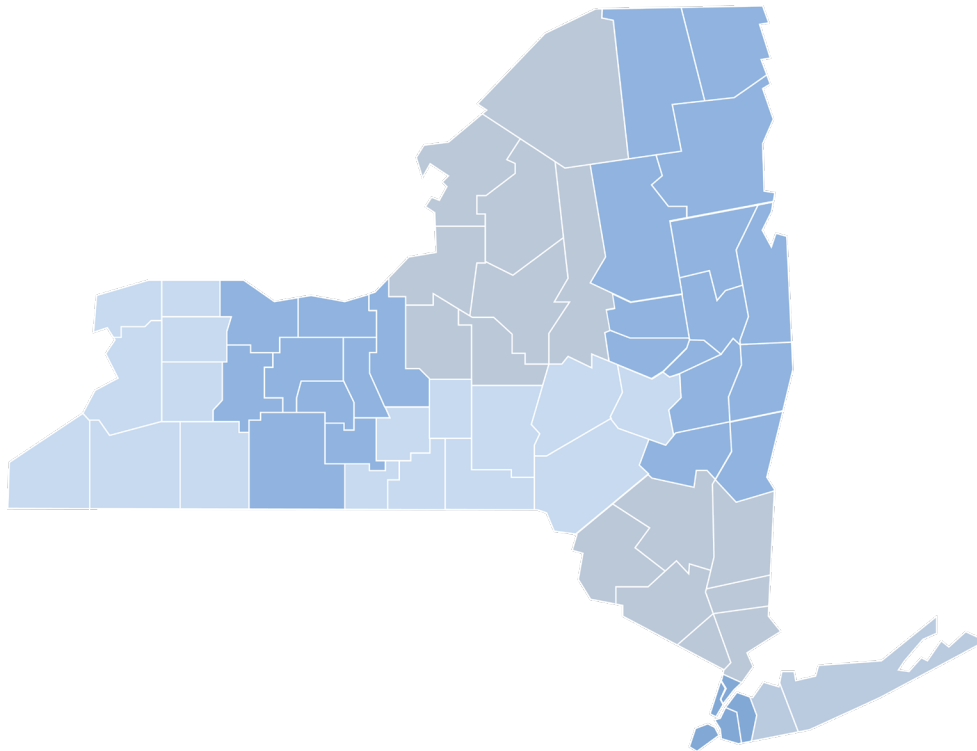
OSC auditors conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that auditors plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on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

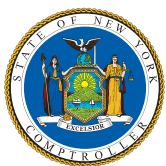
Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or relevant population size and the sample selected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