New York State Comptroller
THOMAS P. DiNAPOLI

Eldred Central School District

Building Access

June 2026 | Report S9-26-1
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 6

Profile 6

Criteria 6

Additional Resources 7

Appendix B: Response From District Officials 8

Appendix C: Audit Methodology and Standards 10

Audit Results

Eldred Central School District

Audit Objective

Did Eldred 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 December 17, 2025 to review access activity logs during our fieldwork.

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 252 active building access accounts (accounts), including 196 devices issued to current employees and 56 issued to non-employees, of which 14 are shared devices.[1] Each of the District's three school buildings has a single public point of entry. Employees and staff may also access the buildings through additional secured entry points, which require a badge 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, the District had active, but unneeded, accounts with assigned badges in the system:

- 14 District employees had two or more active badges, including four employees who were assigned as many as four active badges, one of these employees, the Superintendent of Schools (Superintendent), was assigned seven active badges at the time of our fieldwork in December 2025.
- Seven non-employee badges including five shared badges that were not tracked or disabled when no longer needed and two active badges assigned without a business need to a Board of Education (Board) member and a retired bus driver.
- District officials could not locate 14 active badges, including 13 duplicate employee badges and one shared badge.

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 clearly assign responsibility for managing and monitoring accounts or develop written policies and procedures for issuing and monitoring 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.

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

The Board of Education has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to our office within 90 days, pursuant to Section 35 of 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 your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. The CAP should be posted 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 December 2025, the District had 252 active accounts associated with 196 badges issued to current employees, and 56 badges issued to non-employees including 14 shared badges. We determined:

- 30 percent of current employee accounts had duplicate active badges, and
- 13 percent of non-employee accounts were unneeded.

Employee Accounts – 196 badges were assigned to 138 current employees. Of the 138 employees, 41 employees (30 percent) were assigned two or more active badges, including four employees who were assigned as many as four active badges, and the Superintendent was assigned seven active badges.

We interviewed the four employees that each had more than four active badges (19 badges total) and requested to observe their physical badges. Two employees showed us only their current badge, and a third employee's supervisor told us the employee repeatedly lost badges and was issued new ones each time. The Superintendent was unable to locate one of her seven active badges. Therefore, District officials could not locate seven of the nine additional badges for these four employees. The Superintendent acknowledged that she had multiple active badges and retained them in case of emergency, or if she forgot one of the badges. After our audit inquiry, the Superintendent had five of her badges deactivated, including the badge that she could not locate. However, she told us that in her role as Superintendent, she felt it was necessary to retain a second active badge as a backup in case of an emergency.

Non-Employee Accounts – Of the 56 non-employee accounts, 40 accounts were assigned to non-employees that required access (e.g., law enforcement, student teachers), 14 accounts were assigned to a shared badge (e.g., elevator access, visitor, bus garage) and two active accounts were assigned to a Board member and a retired bus driver. We determined seven of these active non-employee badges (13 percent) including five shared badges and the two active badges assigned to a Board member and the retired bus driver were unneeded.

The Board member was unaware a badge was issued in their name and told us they did not have custody of this badge. District officials could not provide a reasonable explanation why these two accounts were active.

The 14 active shared badges included nine badges which only provided interior elevator access, four visitor badges for substitute teachers and one generic bus garage badge that the Transportation Director told us was damaged and no longer functioned. Officials disabled this badge during our fieldwork.

The high school main office secretary had custody of and monitored the four visitor badges, which she distributed in the morning to substitute teachers working in the District that day, who were expected to return

the badge at the end of the day. We also observed one visitor badge in the high school main office secretary's possession that was not on the active badge listing. Because the District did not have written procedures for staff to follow or a periodic reconciliation of access within the system, District officials disabled this badge but it was not collected. Conversely, a visitor badge was on the active listing, but District officials could not locate it.

When we brought these issues with badges to District officials' attention, the Information Technology (IT) department director reviewed active accounts and deactivated all duplicate accounts, former employee accounts and accounts associated with lost badges, including the lost badges we identified. However, these issues occurred in part due to a lack of clear communication of responsibilities and poorly documented procedures for managing and monitoring building access, including no regular reconciliation of access accounts and devices, which raised the risk of unauthorized entry to District school buildings.

Account Management and Monitoring Procedures – Although District officials created a chain of responsibilities document which described roles of District officials involved in the building access management process, including two IT department employees, the District did not have any written procedures outlining who is responsible for managing and monitoring building access 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, the process for adding access accounts was handled by the Superintendent's secretary (Secretary) who:

- Added 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.
- Added accounts for non-employees including volunteers, or contractors.
- Printed and issued prenumbered badges to employees and non-employees.

The Secretary told us she monitored active accounts and was responsible for lost badge deactivation, as well as collecting, deactivating and destroying badges that were no longer needed due to resignation, retirement or termination. She also reissued badges if necessary (e.g., lost or damaged badges).

Importantly, the Secretary and the two IT department employees had the same administrative rights in the system to make modifications including activating, deactivating or modifying building access. During our audit period the Secretary and the IT department director both made updates and changes to access accounts. However, no one was periodically reviewing active accounts to determine whether all active accounts were needed. We determined that there was lack of communication and misunderstanding between the Secretary and IT department employees regarding who was primarily responsible for processing access updates or changes. 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. Ensure employees do not have duplicate badges.

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 the Town of Deerpark in Orange County, and the Towns of Highland, Lumberland and Tusten in Sullivan County. The District's buildings are located on campuses in the Town of Highland (Junior/Senior/High School building and Bus Garage) and in the Town of Lumberland (Elementary building).

The District is governed by the elected five-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 Secretary the responsibility for managing and monitoring building access accounts. The Secretary utilizes the system to print and issue badges to users which are then distributed either by her or department heads. The IT Director and an IT 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 guidance[2] provides that, as the second line of defense when protecting 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[3] 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, 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.

2 https://www.nysed.gov/sites/default/files/programs/facilities-planning/safeschoolsbydesign-aguidebynysed-april2025.pdf
3 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 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)*,[4] and may have included changes to spelling and grammar. The substance of the content was not changed.

Mrs. Traci Ferreira, Superintendent of Schools
600 Route 55, PO Box 249, Eldred, N.Y. 12732
Tel: 845.456.1010 Fax 845.456.1113
Email: ferreirat@eldred.k12.ny.us

May 27, 2026
Nicole A. Tomsen, Chief of Municipal Audits
Division of Local Government and School Accountability
110 State Street
Albany, NY 12236

Re: Response to the Draft Report of Examination S9-26-1 Building Access Audit

Dear Ms. Tomsen:

The Eldred Central School District acknowledges receipt of the Draft Response of Examination S9-26-1 Building Access Audit for the period covering July 1, 2025 through December 17, 2025. On behalf of the Board of Education and administration, we appreciate the opportunity to respond in kind with a narrative regarding the finding of the draft report.

The Eldred Central School District recognized in July of 2025 that we needed to review our policies and procedures for creating, issuing, and destroying building access badges. Upon receiving the audit data, the district took swift action to resolve all immediate vulnerabilities regarding active access badges. The audit identified 41 district employees with two or more active badges. All secondary badges have been located, deactivated in our system, and physically destroyed. The only individual currently authorized to hold two active badges is the Superintendent of Schools, required for distinct operational and security oversight roles. Seven active badges assigned to non-employees were immediately deactivated. Any badges that could not be physically located during this review were immediately deactivated in the system and officially logged as lost.

While the district previously maintained a standard process for adding employee, contractor, and vendor accounts, we recognize the need for more rigorous lifecycle management of these credentials. The following protocols have now been established. The Director of Technology, in coordination with the Human Resources Secretary and the Superintendent of Schools, conducted a full audit of the system database. All duplicate accounts, former employee accounts, and accounts tied to lost badges have been permanently deactivated. To mirror our existing onboarding protocol, the district has officially initiated a formal off-boarding process. This ensures that when an employee, contractor, or vendor leaves the district, their access badges are systematically deactivated and collected without delay. The Superintendent, Administrative Cabinet, and Director of Technology reviewed all system access groups. We have established strict, standardized access parameters tailored specifically to the requirements of each employment position.

The Director of Technology and the Administrative Cabinet will review all badge access parameters annually. This mandatory annual review will incorporate a rigorous reconciliation process across all user groups to ensure accounts are actively managed, monitored, and aligned with our strict building security protocols.

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

The district remains committed to maintaining a secure environment and believes these decisive steps will prevent future discrepancies while hardening our overall facility security. The district will submit a Corrective Action Plan in a timely manner. This Corrective Action Plan will illustrate and go into detail the changes that were made at the initiation of the 2025-2026 school year. The Eldred Central School District appreciates the hard work, effort, communication and transparency with the auditors throughout the entirety of this process.

Respectfully,

Traci Ferreira
Superintendent of Schools

Appendix C: Audit Methodology and Standards

We obtained an understanding of internal controls that we 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 building access accounts and badges, including roles and responsibilities of the individuals involved in the process.

- We compared the District's 252 active building access accounts list to the employee master list of 152 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 selected all 14 shared and generic accounts 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.

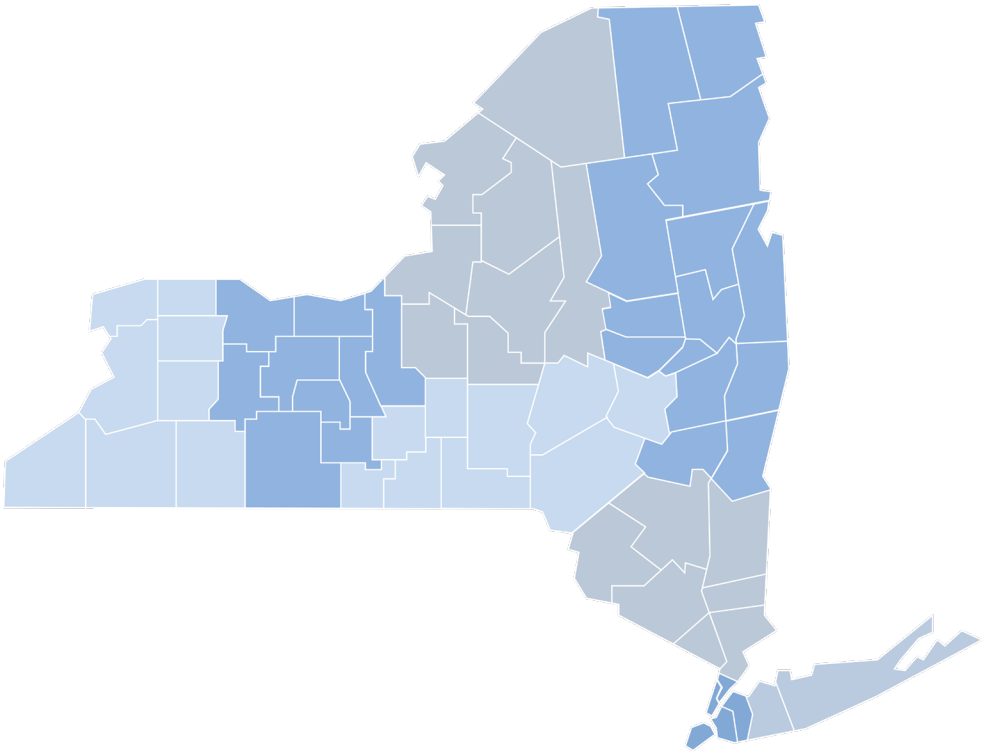
- We reviewed the active building accounts list to determine whether any users had more than one account and badge and interviewed District officials to determine why users were assigned more than one account. We identified 41 employees with a total of 57 duplicate badges. We judgmentally selected four employees with four or more duplicate accounts totaling 19 badges. We followed up with each employee to observe all badges in their possession and determine why they had multiple access accounts and badges.

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

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