New York State Comptroller
THOMAS P. DiNAPOLI

Auburn Enlarged City School District

Building Access

July 2026 | Report S9-26-13
Prepared by the Division of Local Government and School Accountability

Table of Contents

Audit Results

Auburn Enlarged City School District

Audit Objective

Did Auburn Enlarged City 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 January 29, 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 1,276 active building access accounts (accounts), including 828 devices issued to current employees and 448 issued to non-employees, of which 137 are shared devices.[1] Each of the District's eight school buildings has 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 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:

- 26 District employees and one non-employee had two active badges each.
- 32 percent of individual non-employee accounts reviewed were not disabled when no longer needed.
- 56 percent of shared badges issued did not comply with the District's building management procedures.
- 85 percent of shared badges we reviewed were unneeded.

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. These issues occurred because District officials did not follow the written procedures that clearly described and assigned responsibilities to District officials for managing and monitoring accounts, as well as issuing and monitoring 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 five 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 your CAP, please refer to the OSC 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 February 2026, the District had 1,276 active accounts associated with 828 badges assigned to 802 current employees, and 448 badges issued to 311 non-employees including 137 shared badges. We determined:

- 3 percent of current employee accounts had duplicate active badges,
- 32 percent of individual non-employee accounts we reviewed were unneeded,
- 56 percent of shared badges issued did not comply with the District's building management procedures, and
- 85 percent of shared badges we reviewed were unneeded.

Employee Accounts – Of the 802 current employees, 26 employees (3 percent) were assigned two active badges, including the Superintendent. We reviewed four of the 26 employee accounts that had two active badges, including the Superintendent, to determine why more than one active badge was assigned. We determined that:

- Two duplicate badges were issued as replacements because the original badges were damaged. However, the original badges were not properly disabled.
- One duplicate badge was assigned to an Information Technology (IT) department staff member to test building access. The Director of Technology (Director) told us he did not know the test badge existed and that the badge was not needed.
- The remaining badge reviewed was assigned to the Superintendent. She told us the duplicate badge was only kept for building lockdown emergencies and felt that the badge was necessary for her role.

We verified that the replacement duplicate badges and the duplicate badged issued to test building access were properly deactivated prior to the completion of our fieldwork. Although officials determined the Superintendent's duplicate badge was needed, retaining duplicate active badge increases the risk of lost or stolen devices and unauthorized entry to District school buildings.

Non-Employee Accounts – 311 accounts were assigned to individual non-employees such as first responders, contractors or other individuals (e.g., various service providers, coaches) and 137 accounts were assigned to a shared badge. We reviewed 25 of the 311 individual non-employee accounts and determined that eight of the 25 (32 percent) accounts and badges were assigned to third-party individuals who no longer performed services for the District and were therefore no longer needed.

According to the District's building management procedures, non-employees must receive approval from the building principal, personnel department and Superintendent to receive a badge. To deactivate an account and badge, the IT department requires notification from a department head through the help desk system when a

non-employee no longer needs building access. The Director told us the IT department did not receive notification to deactivate the eight badges. Therefore, these badges remained active and potentially used for unauthorized access. During our fieldwork, the Director deactivated the unneeded badges and we verified that all eight non-employee badges were disabled.

Additionally, the Director, also a non-employee, had two active badges. As with some of the duplicate employee badges we reviewed, the Director's duplicate badge was issued as a replacement because his original badge was damaged but the original badge was not disabled. We brought this to the Director's attention, and he deactivated his duplicate badge.

Of the 137 active shared badges, 60 were for first responders which the Director told us were needed for law enforcement. However, the remaining 77 badges (56 percent), issued for various roles such as coaches, contractors, substitutes and interns, did not comply with the District's building management procedures and District officials should not have issued them. Of the 77 badges, seven were never used, and 16 badges were not used in at least three years. We also reviewed 13 of the 77 shared badges to determine their purpose. We determined 11 badges (85 percent) were not needed. Specifically:

- Six shared badges overseen by the Athletics department's assistant (assistant) were provided to coaches. The assistant did not know where four of the badges were located. Of the remaining two badges, one badge was provided to a coach, who was also a District employee that already had an individual badge. This employee used both badges to access school buildings. The remaining badge was provided to a non-employee coach, and the badge was not returned to the District when the coaching season was completed.
- Two shared badges were provided to former contractors who no longer performed services in the District.
- One shared badge was provided to the mail service vendor. The Director told us the badge was provided for convenience but was not needed.
- The two remaining shared badges were issued to an intern and a substitute secretary who no longer performed services at the District.

Neither the Athletic nor the Facilities departments' officials knew which coaches or contractors under their direction had active badges until we provided a list of badges for their review. Neither department's officials notified the IT department that the badges were no longer needed. Furthermore, according to District building management procedures, officials should have assigned all of these badges to an individual non-employee account.

District officials told us that the remaining two of the 13 badges were needed for an active coach and a BOCES inspector. Although these badges were needed, according to District building management procedures, officials should have assigned the badges to an individual non-employee account.

During fieldwork, the Director told us that he began to deactivate the unneeded shared badges we identified in this report. We verified that all 11 badges were disabled during our fieldwork.

Account Management and Monitoring Procedures – District officials established written procedures that clearly define who is authorized to create building access accounts, who can receive a badge and the limits of access (i.e., time period or locations necessary for job-related duties). These procedures also define who is responsible for monitoring active accounts and the process to revoke access by deactivating unneeded accounts and collecting badges. However, District officials did not always follow these procedures because, as we identified earlier in this report, the District had unnecessary badges, and 56 percent of shared badges issued did not comply with the District's building management procedures.

The Director told us that the procedures were created in August/September 2025 as a corrective action following a cybersecurity audit. He also told us that the procedures were not provided to all key individuals because District officials were still finalizing them and, as a result, some District staff were unaware of the District's procedures. Additionally, the IT department did not periodically review active accounts to determine whether the accounts were needed.

Because District staff were unfamiliar with the building access procedures, account updates including deactivation of unneeded badges were not always made in a timely manner. This resulted in a potential for unauthorized access to District buildings.

Recommendations

District officials should:

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

2. Ensure individuals do not have duplicate badges.

3. Ensure every individual (employee, vendor, contractor, or other authorized user) is assigned a unique and individual badge.

4. Provide the building access management procedures to key individuals involved in the process and periodically evaluate and adjust these procedures to ensure all processes are working as intended.

5. Develop a reconciliation process utilizing system reports, and review active badges for necessity and appropriateness of access.

Appendix A: Profile, Criteria and Resources

Profile

The District's boundaries include the City of Auburn and parts of Towns of Aurelius, Fleming, Owasco and Sennett in Cayuga County. The District's buildings are located on campuses in the City of Auburn.

The District is governed by the elected nine-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 IT department is responsible for managing and monitoring building access accounts. The IT department utilizes the system to print and issue badges to users which are then distributed by department heads. The IT Director and IT department staff members have administrative rights to activate, modify and deactivate accounts in the system.

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.

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

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

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, 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.

Auburn Enlarged City School District

Nicole A. Tomsen, Chief of Municipal Audits
Office of the State Comptroller
Division of Local Government and School Accountability

Re: Auburn Enlarged City School District – Building Access Audit (Draft Report S9-26-13)

July 6, 2026

Dear Ms. Tomsen:

The Auburn Enlarged City School District appreciates the professionalism and collaboration demonstrated by the Office of the State Comptroller throughout the building access audit process. District officials have reviewed the preliminary draft report and generally agree with the findings and recommendations.

The audit provided the District with an opportunity to evaluate and strengthen its building access management practices. While the District had established procedures governing employee and non-employee access during the audit period, the review identified areas where oversight, communication, documentation, and periodic review processes could be improved.

District officials have already implemented numerous corrective actions during and immediately following the audit fieldwork. At the auditors' request, duplicate, unnecessary, and inactive badges identified during testing were reviewed and deactivated. This included athletic badges, contractor badges, food service badges, mail service badges, substitute badges, duplicate employee badges, testing badges, and other credentials determined to no longer have a valid business purpose. District officials provided documentation and screenshots to the audit team confirming these actions throughout the course of the audit.

In addition, the District completed a comprehensive review of non-employee access, including coaches, contractors, service providers, and other third-party badge holders. Departmental reviews were conducted to validate active access and remove credentials no longer needed. The District also reviewed duplicate badges assigned to employees and implemented procedures to ensure replacement badges are properly disabled when new credentials are issued.

To further strengthen governance, the Board of Education adopted a Building and Door Access Control Policy in May 2026. The policy establishes clear accountability, authorization requirements, individual badge assignment standards, periodic review requirements, and oversight responsibilities for building access management. The District also developed a companion Administrative Regulation that formalizes procedures for onboarding, special access requests, non-employee access, termination processing, monitoring, and reporting.

The District has implemented a standardized electronic Door Access Control Request Form and workflow to document all access requests, approvals, modifications, and removals. Furthermore, the District established a bi-annual reconciliation and review process involving the Information Technology Department and designated

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

departmental contacts responsible for non-employee access, including Athletics, Facilities, Food Service, Student Services, and other operational areas.

As a result of the audit, the District has strengthened communication expectations regarding employee separations, non-employee access approvals, badge issuance, and access revocation. These improvements will help ensure that access remains appropriate, documented, and periodically reviewed.

District officials appreciate the recommendations contained in the report and believe the corrective actions already completed place the District in a strong position moving forward. The District will continue to evaluate and improve its building access management program and looks forward to submitting its formal Corrective Action Plan following issuance of the final report.

Sincerely,

Misty L. Slavic, Ed.D.

Superintendent of Schools

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 1,276 active building access accounts list to the employee master list of employees to determine whether active accounts were associated with current District employees, non-employees or were shared accounts. Of the 311 active individual accounts that were not assigned to an employee, we selected 25 accounts to determine whether the accounts were necessary. For any unnecessary accounts, we interviewed District officials and reviewed relevant documentation to inquire as to why the accounts were not deactivated.

- We selected 13 of the 137 shared accounts and inquired with the respective District officials responsible for these badges to determine whether the badges were necessary and in their possession. For any unnecessary accounts, we inquired as to why they were not deactivated. If the badges were not in the officials' possession, we inquired to determine why and attempted to locate the badges.

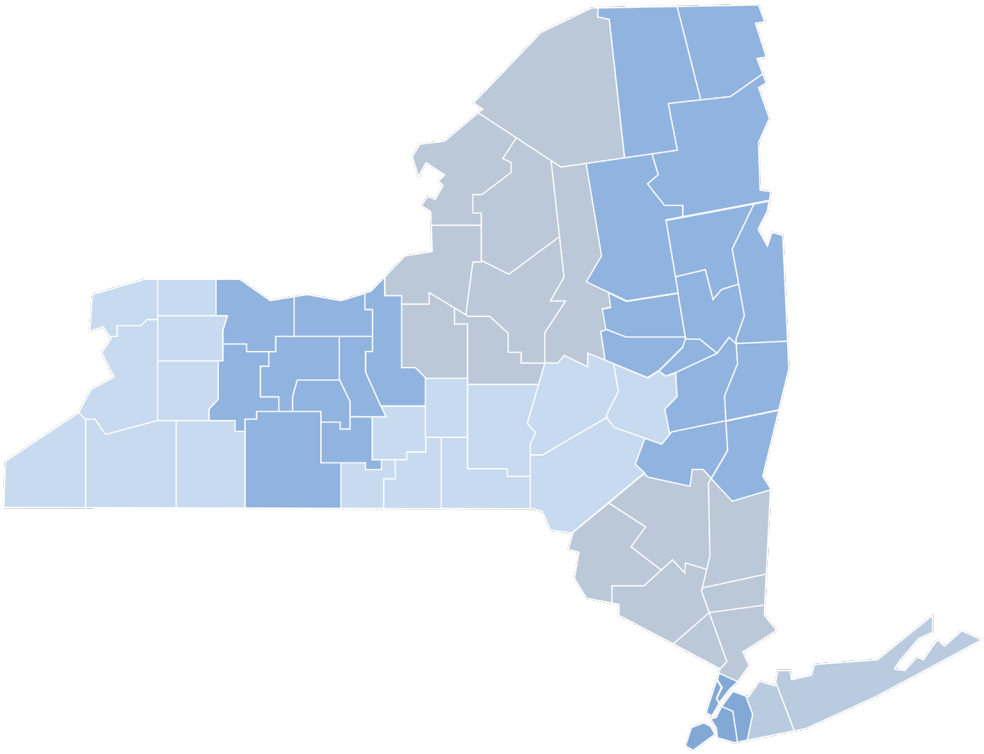
- We reviewed the active building accounts list to determine whether any users had more than one account and badge and interviewed District officials to determine why individuals were assigned more than one account. We identified 27 individuals (26 employees and one non-employee) with a total of 54 duplicate badges. We randomly selected two employees and used our professional judgment to select an additional two employees and one non-employee who were involved in the building access management process with duplicate badges totaling 10 badges. We followed up with District employees to determine why users had multiple access accounts and 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