New York State Comptroller
THOMAS P. DiNAPOLI

Batavia City School District

Building Access

July 2026 | Report S9-26-10

Prepared by the Division of Local Government and School Accountability

Table of Contents

Audit Results

Batavia City School District

Audit Objective

Did Batavia 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 22, 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 749 active building access accounts (accounts), including 601 access devices issued to current employees and 191 issued to non-employees, of which 35 are shared devices.[1] Each of the District's five 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 (key fobs). 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 key fobs in the system:

- 16 District employees had a total of 34 active key fobs, including one employee who was assigned four active key fobs.
- Seven non-employee key fobs we identified were not deactivated when no longer needed.
- Four shared key fobs, which District officials could not locate and had no record of whom they were provided to, were not deactivated.

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 in part because District officials did not establish written procedures that clearly assigned who was responsible for managing and monitoring accounts or develop written policies and procedures for issuing and monitoring key fobs.

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 key fobs. District officials agreed with our recommendations and have initiated or indicated they planned to initiate corrective action.

This audit was conducted pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's (OSC'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 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 key fobs.

During our fieldwork in January 2026, the District had 749 active accounts associated with 792 key fobs. These included 601 key fobs issued to 583 current employees, and 191 key fobs issued to 46 individual non-employees and 35 shared key fobs. We determined:

- 16 (3 percent) current employee accounts had duplicate active key fobs,
- Seven (15 percent) individual non-employee accounts we identified were unneeded,
- Four (33 percent) of the 12 active shared key fobs assigned to the primary school could not be located by District officials.

Employee Accounts – Of the 583 employees, 16 employees (3 percent) were assigned a total of 34 active key fobs, including one employee who was assigned four active key fobs. The Director of Facilities (Director) and Assistant Director of Facilities (Assistant Director) told us that duplicate key fobs were issued to nine custodial employees for the convenience of having a key fob on both employees' personal keyring and their District keyring. However, their job duties did not require multiple key fobs. One of the custodial employees was issued four key fobs. Further, the Director and Assistant Director each retained two active key fobs which they felt was necessary as a backup in case of emergency.

District officials could not explain why the remaining five employees were assigned more than one key fob. Of the duplicate active key fobs assigned to the five employees, two were never used and two were lost or damaged. The remaining active key fob had an expiration date configured for January 2025 (approximately six months into our audit period) which overrode its active status; as of the expiration date, the key fob no longer allowed access to District buildings.

When we brought these issues to District officials' attention, the Assistant Director told us that the District deactivated these five employees' additional active key fobs and we confirmed this during our fieldwork. However, the Director's and Assistant Director's additional active key fobs, along with those of the other nine employees, remained active. Allowing unnecessary duplicate key fobs increases the risk of lost or stolen key fobs and unauthorized entry to District school buildings.

Non-Employee Accounts – For the individual non-employee accounts, we sampled and reviewed 10 of the 46 accounts with District officials,[2] and reviewed personnel changes as documented in August through December 2025 Board meeting minutes. We determined that seven active individual non-employee accounts (15 percent) were unneeded. Specifically:

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

- Two of the 10 accounts we sampled and reviewed with District officials were assigned to former employees who separated from the District in June 2009 and August 2024, but were not disabled. After our audit inquiry, District officials disabled these accounts and key fobs.
- Five accounts for former employees who left District employment between August through December 2025 as documented in the Board meeting minutes remained active. District officials could not provide a reasonable explanation why these accounts remained active.

The Assistant Director told us that he implemented a control in which the system would automatically disable any key fobs that are not used for six months. However, we observed that this control was not operating effectively. For example, we identified a key fob that remained active for a former employee who had not used it since his separation from District employment in August 2024; 17 months prior to the start of our audit. District officials should disable employees' accounts as soon as they are no longer needed to prevent unauthorized access to District school buildings.

The 35 active shared key fobs were for substitute employees, such as teachers and custodians. Officials told us that designated District employees had custody of these key fobs when they were not in use, such as the main office secretaries for each building. We reviewed the 12 shared key fobs at the primary school main office, and District employees and officials were unable to locate four of the active key fobs. Officials did not maintain a written log or any other record to track who the four shared key fobs were provided to, diminishing accountability and limiting the ability to detect loss or potential misuse. Additionally, District officials did not deactivate the four key fobs after we brought this to their attention because they believed the key fobs were needed and were in the possession of substitutes.

Because the District did not have written procedures for staff to follow or a periodic reconciliation of access, there is a risk that shared key fobs are not collected. Additionally, there were no procedures for the supervisors of the substitute employees or the main office secretaries to track or collect shared key fobs each day.

<u>Account Management and Monitoring Procedures</u> – District officials did not establish procedures clearly assigning the roles and responsibilities of all parties involved in the building access management process or have any written procedures outlining who is responsible for managing and monitoring accounts. Specifically, the District 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 key fobs. At the time of our audit in January 2026, the process for adding individual employee accounts was handled by the facilities department's 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, as provided by the human resources department.
- Issued prenumbered key fobs to employees.
- Deactivated lost key fobs, as well as collected, deactivated and destroyed key fobs that were no longer needed due to resignation, retirement or termination.
- Reissued key fobs if necessary (e.g., lost or damaged key fobs).

The Assistant Director was responsible for adding accounts for non-employees including contractors, substitutes and first responders and monitoring active accounts. The Assistant Director told us that he monitored active accounts by utilizing daily system reports as well as relying on the system control that was designed to automatically deactivate accounts after six months of inactivity. However, no one was periodically reviewing active accounts to determine whether all active accounts were needed or whether the deactivation control was operating effectively.

Based on our audit testing, we determined that the system deactivation control was not effective, and that there was lack of communication between the human resources department and the facilities department regarding the need for access, updates, changes or deactivation. As a result, account updates were not always made in a timely manner and there was a potential for unauthorized access to District buildings.

Recommendations

District officials should:

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

2. Ensure employees do not have duplicate accounts and key fobs.

3. Develop written procedures that define who is responsible for managing and monitoring accounts including shared key fobs and periodically evaluate and adjust these procedures to ensure all processes are working as intended.

4. Develop a periodic 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 City of Batavia and the Towns of Batavia and Stafford in Genesee County. The District's buildings are located on campuses in the City of Batavia.

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 Assistant Director is responsible for managing and monitoring accounts by utilizing the system and oversees the facilities department's secretary who is responsible for issuing key fobs to individuals which are then distributed either by her or department heads. The Assistant Director also has 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[3] 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 Guide[4] recommends schools should have in place a layered, system-based approach to physical security in which physical security equipment and technology, site and building features, personnel and staff, policies and procedures, and training programs work together to ensure school facilities are secure.

Policies and Procedures – Schools should develop and implement physical security and access control policies and procedures with roles and responsibilities defined and assigned across its organizational entities (e.g., IT, Human Resources (HR), administration, facilities etc.). Policies and procedures should be established to manage, monitor and revoke building access devices and other access credentials as necessary. The policies and procedures should be periodically reviewed and updated to reflect the current and approved access controls implemented within the system and organization.

Building Access/Entry – Schools should control who can enter school buildings, where they can go, and when access is permitted. Building access systems serve as an internal control to help ensure safety and security including controlled entry points, visitor management and monitoring building access. Internal controls over building access/entry should be designed in a way that primary entrances are controlled through device readers, security desks or locked-door systems.

Building Access Account Management – Only designated system users/administrators should be able to create, enable, modify, revoke and remove accounts in accordance with documented policies and procedures. System administrators for access management should be limited and have clearly defined roles and responsibilities. Account management processes should align with individual status changes, such as extended leave, termination or other circumstances when access is not required.

Device Issuance and Authorization – Devices should only be issued with documented approval based on job role and building assignment, each device should be unique and individually assigned. Each individual should 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, 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.

Batavia City School District
Jason A. Smith, Superintendent
260 State Street, Batavia, NY 14020
Phone: (585) 343-2480
Email: jasonsmith@bataviacsd.org

July 21, 2026

Nicole Tomsen, CIA
Chief of Municipal Audits, Statewide Audits
Division of Local Government & School Accountability
295 Main Street, Suite 1032,
Buffalo, New York 14203-2510

Dear Ms. Tomsen:

We wish to acknowledge the receipt of the findings and recommendations outlined in your "Building Access Report S9-26-10" of the Batavia City School District for the period of July 1, 2024-November 30, 2025.

Our District takes this report seriously as well as the safety of our students and staff. We value the constructive recommendations offered by the Office of the New York State Comptroller included in this report.

We accept the findings outlined in this report and wish to provide additional context around the audit findings, with the understanding that this context is in no way an excuse or an attempt to evade responsibility.

- During the audit period there was administrative and clerical turnover in the Human Resources office which made it difficult to develop a consistent process for the deactivating and collecting of fobs.
- The turnover in the Human Resources office also prevented the development of a clear written procedure for the deactivation of fobs assigned to former employees.
- It should be noted that the audit found that there were only 5 fob accounts from former employees which were not deactivated from August 2025 through December 2025. This represents 0.6% of the total number of issued fobs (792).

Additionally, we wish to submit that the District has already addressed the findings as follows:

- We have deactivated and collected fobs that are duplicate or not needed
- We have created a written procedure for activating and deactivating employee fob access including periodic monitoring

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

The Batavia City School District would like to thank the Office of the New York State Comptroller and their audit team for their professionalism and collegiality during the audit process. This report provided valuable feedback to help improve our safety practices, which allows us to continue to provide a safe learning environment for our students and a safe workplace for our faculty and staff.

John Reigle President, Board of Education	Jason Smith Superintendent of Schools	Andrew Lang Business Administrator

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 accounts and key fobs, including roles and responsibilities of the individuals involved in the process.

- We compared the District's 749 active accounts list to the employee master list of 739 employees to determine whether accounts existed that were not associated with current District employees. We identified 46 active accounts that were issued to individual non-employees and used a random number generator to select a sample of 10 active individual non-employee accounts. We interviewed District officials and reviewed relevant documentation to determine whether the accounts and key fobs assigned to non-employee individuals were necessary. For any unnecessary accounts, we inquired as to why they were not deactivated.

- We reviewed Board meeting minutes from August to December 2025 for resignations, retirements and terminations and traced the individuals who were no longer employed by the District to the active accounts to determine whether they retained an active key fob.

- We identified 35 shared accounts and inquired with the respective District officials responsible for the associated key fobs to determine their purpose, whether they were in their possession, and whether the officials maintained a written log to track usage of these key fobs.

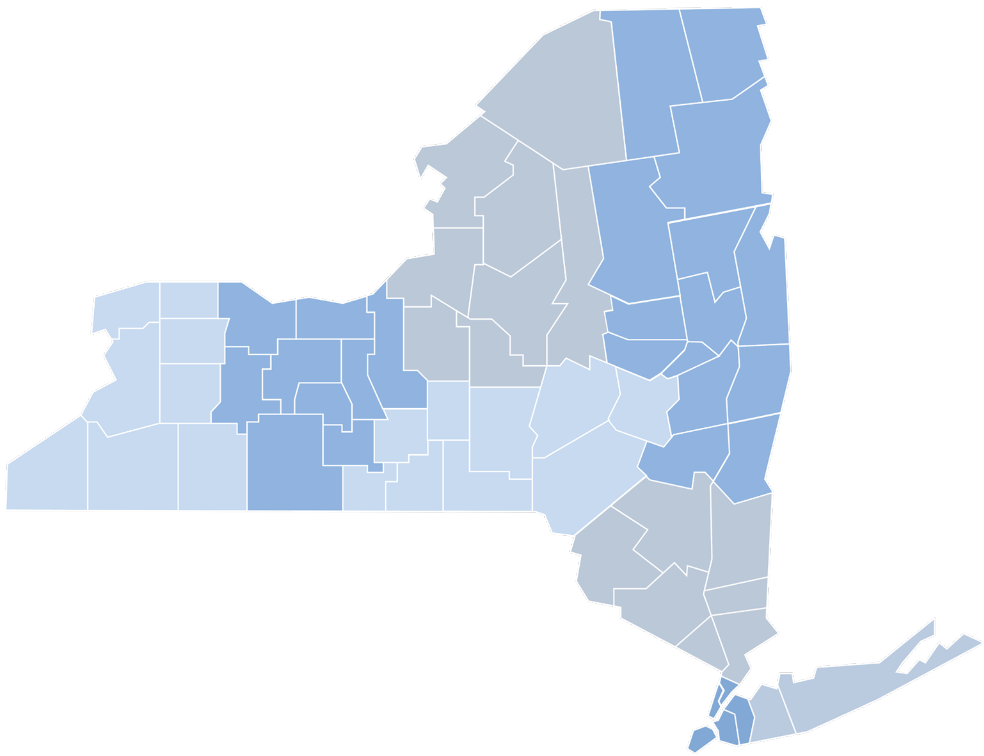
- We reviewed the active accounts list to determine whether any individuals had more than one account and identified 16 employees who were assigned to a total of 34 access accounts and key fobs. We interviewed District officials and reviewed their last access information to determine why these employees were assigned multiple accounts and key fobs.

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

https://www.osc.ny.gov/

Prepared by the Division of Local Government and School Accountability

NYS FOLLOW US: osc.ny.gov/subscribe