New York State Comptroller
THOMAS P. DiNAPOLI

Broadalbin-Perth Central School District

Building Access

August 2026 | Report S9-26-5
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 5

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 11

Audit Results

Broadalbin-Perth Central School District

Audit Objective

Did Broadalbin-Perth 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 February 27, 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 477 active building access accounts (accounts) associated with 395 devices issued to current employees, and 82 issued to non-employees including 56 shared devices.[1] Each of the District's two school buildings have 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, the District had active, but unneeded, accounts with assigned badges in the system:

- 12 District employees had at least two active badges.
- 42 shared non-employee badges without expiration dates were not monitored to ensure they were still needed and accounted for, including 23 badges that were either never used or not used in at least a year.

These issues occurred because District officials did not establish clear, written procedures assigning responsibility for issuing, managing and monitoring accounts. District officials implemented a process for adding accounts for employees and non-employees and deactivating employee accounts upon retirement, resignation or termination. Non-employee accounts were automatically disabled using expiration dates if a non-employee badge request form was received. However, the form was not always used, and no one routinely reviewed all active accounts to confirm their necessity. District officials generally agreed with our recommendations and their response is included in Appendix B.

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.

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 C.

The Board of Education (Board) has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to OSC within 90 days, pursuant to Section 35 of GML, Section 2116-a (3)(c) of the New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. For more information on preparing and filing the CAP, please refer to the OSC brochure, *Responding to an OSC Audit Report*, which was provided with the draft audit report. The CAP should be posted on the District's website for public review.

Building Access: Finding and Recommendations

Properly managing and monitoring building access is a fundamental security function and the responsibility of school district officials. Various resources, publications, and guides are available to help school district and Board of Cooperative Educational Services (BOCES) (together, "schools") officials develop and implement necessary building access infrastructure and systems to create a safe and secure environment for their students, teachers, staff and visitors.

To issue accounts and badges for non-employees, the District used a badge request form that required:

- Details about the individual requiring a badge including their name, title, phone number and address, as well as access needs including the building(s) days and hours, and an expiration date for end of access.
- An authorizing signature from the Superintendent.

More details on the building access management and monitoring criteria used in this report as well as resources we make available to local officials that can help officials 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 477 active accounts associated with 395 badges issued to 382 current employees, and 82 badges issued to non-employees, including 56 shared badges. We determined:

- 12 current employee accounts had duplicate active badges, and
- District officials did not monitor or review for necessity any of the 42 shared accounts and badges we reviewed, including 23 badges that were either never used or not used for at least a year.

Employee Accounts – Of the 382 employees, 12 employees (3 percent) were assigned two or more active badges, including the Superintendent with three active badges and the Assistant Superintendent with two active badges.

The Human Resources Clerk (Clerk) told us that nine of these duplicate badges were due to employees not returning previous badges for deactivation when she issued new badges to all employees at the beginning of the 2025-26 school year. The Clerk deactivated the duplicate badges for these nine employees during our fieldwork. One other employee had two active badges assigned to them due to a recent change in position; however, the employee only had possession of the previous position's badge. The Clerk told us that she activated the badge for the employee's new position and would deactivate the older badge when they picked up the new one. Although we observed that the new badge was locked in the Clerk's desk still awaiting pickup, each individual should only have one device and any replacement badge should not be activated until the older badge is returned.

After our audit inquiry the Clerk deactivated the Superintendent's oldest badge. However, District officials justified the need for the Superintendent and the Assistant Superintendent to have two badges, due to their positions and potential emergency response needs that may arise.

Non-Employee Accounts – We reviewed 42 of the 56 active accounts with shared badges issued to third parties (20 to the police department, 15 to a construction company for an ongoing capital project, and seven to a bank for servicing the ATM in the Junior-Senior High School). The Clerk told us the District issued these

badges before it began using the badge request form and implementing its requirements for non-employee access. Therefore, no access expiration dates were set for any of the badges. However, we determined District officials did not monitor them to ensure they were all physically accounted for and still needed. Further, based on usage data we reviewed, 23 of these badges (55 percent) were either never used or not used in at least a year. Specifically:

- Only one of the police department badges was used in the past year (in September 2025), 10 badges were not used in at least a year, and nine badges were never used. While officials indicated that these badges were still necessary, they have not reviewed them with the police department to ensure they are all accounted for and needed.
- The 15 badges assigned to the construction company were last used in August 2025 or more recently. Based on our inquiry, the Clerk told us she confirmed these badges were accounted for and still necessary.
- Of the seven badges assigned to the bank, four were never used, and the other three were used in October 2025 or more recently. The Clerk deactivated the four unused badges during our fieldwork and told us the bank remains responsible for them. However, when District officials allow a vendor to manage access to District buildings, it increases the risk that individuals unaffiliated with the District could gain unauthorized access.

Although District officials provided a reason for why these badges were originally issued, no one periodically communicated with those third parties to ensure the badges were still in their possession and accounted for. Having active badges assigned to third parties that have never been used, or not used in over a year, could indicate they are no longer needed. Furthermore, unaccounted for badges that do not expire increases the risk of unauthorized entry to District school buildings.

Account Management and Monitoring Procedures – We verified that the information on the badge request forms for a sample of two non-employees matched the information in the badge system, including expiration dates, building locations and hours, and were signed by the Superintendent for authorization, to confirm the process was operating effectively. However, the District did not have any written procedures outlining who is responsible for managing and monitoring accounts. Specifically, District officials did not define who is authorized to create accounts and who is responsible for monitoring active accounts. District officials also did not outline the process to revoke access by deactivating unneeded accounts and collecting badges (unless a non-employee badge request form was used). At the time of our fieldwork, the process for adding access accounts was handled by the Clerk 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. These accounts were created after the Clerk processed their employment paperwork.
- Added accounts for non-employees (for example, volunteers, police or contractors), based on information included in the badge request form, after she verified that the forms were signed and approved by the Superintendent.
- Printed and issued prenumbered badges to employees and non-employees.

The Clerk told us she monitored active access accounts at the end of the school year by ensuring accounts were deactivated for retirees and other individuals who were no longer employees, as well as reviewing the badge request forms for expiration dates to ensure access was removed as planned. She told us she was also responsible for lost badge deactivation, as well as collecting, deactivating and destroying badges that were no longer needed. She also issued new badges if necessary (e.g., lost or damaged badges).

However, no one was periodically reviewing all active accounts, to determine whether they were needed. As a result, there were duplicate employee badges still active and non-employee badges that may not be needed, creating a potential for unauthorized access to District buildings.

Recommendations

District officials should:

1. Ensure employees do not have duplicate badges.

2. Use the badge request form for all non-employee badge access provided.

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

4. 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.

5. 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 Towns of Broadalbin, Johnstown, Mayfield, Northampton and Perth within Fulton County, the Town of Amsterdam within Montgomery County, and the Towns of Edinburg, Galway, and Providence in Saratoga County. The District's buildings are located on campuses in the Town of Amsterdam (elementary school building) and in the Town of Broadalbin (junior/senior high school building and the District office/transportation building).

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 Clerk the responsibility for managing and monitoring building access accounts. The Clerk utilizes the system to print and issue badges to individuals which are then distributed by her. The Business Manager also has administrative rights to activate, modify and deactivate accounts if the Clerk 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 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[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 (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.

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's 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.

Broadalbin-Perth Central School District
Ashley Brooks
School Business Manager
brooksa@bpcsd.org

Corrective Action Plan
Broadalbin-Perth Central School District
OSC Audit Report - Building Access
Report S9-26-5
July 20, 2026

The Broadalbin-Perth Central School District has received the New York State Office of the State Comptroller audit report titled *Building Access.* The report contains recommendations intended to strengthen the District's management and monitoring of building access accounts and badges. Please accept the following as the District's official Corrective Action Plan. In accordance with the audit report, the District has addressed each recommendation individually and identified the planned corrective actions, implementation dates, and responsible officials.

Recommendations and Corrective Actions

Recommendation #1:

Ensure employees do not have duplicate badges.

Implementation Plan of Action(s):

The District has reviewed all active employee badge assignments and deactivated unnecessary duplicate badges identified during the audit. Going forward, replacement badges will not be activated until the previously issued badge has been returned and deactivated, unless an operational need has been approved by the Superintendent. The Human Resources Clerk will monitor badge issuance to ensure each employee is assigned only one active badge.

Implementation Date:

Completed April 1st, 2026, ongoing monitoring.

Person Responsible:

Caitlyn Vivacqua, Human Resources Clerk

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

Recommendation #2:

Use the badge request form for all non-employee badge access provided.

Implementation Plan of Action(s):

The District will require that all non-employee building access requests be submitted using the District's Non-Employee Badge Request Form. The form will be completed in full, approved by the Superintendent, and include the individual's affiliation, authorized building access, approved days and times of access, and an expiration date. No non-employee badge will be issued without an approved request form.

Implementation Date:

Completed April 1st, 2026, ongoing monitoring.

Person Responsible for Implementation:

Caitlyn Vivacqua, Human Resources Clerk

Recommendation #3

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

Implementation Plan of Action(s):

The District will ensure that employee and non-employee building access accounts are deactivated and badges are collected immediately upon separation of employment, completion of contracted work, expiration of approved access, or whenever access is no longer required. Lost or stolen badges will be deactivated immediately upon notification. Badge returns and deactivations will be documented as part of the District's offboarding and access management procedures.

Implementation Date:

Completed April 1st, 2026, ongoing monitoring.

Person Responsible for Implementation:

Caitlyn Vivacqua, Human Resources Clerk

Recommendation #4:

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.

Implementation Plan of Action(s):

The District will develop and implement written procedures governing the administration of the building access system. The procedures will identify responsibilities for issuing, modifying, monitoring, reconciling, and deactivating employee and non-employee badges, including shared badges. The procedures will also establish requirements for documenting badge issuance, reporting lost badges, collecting badges upon separation, and periodically reviewing the effectiveness of the District's building access controls. The procedures will be reviewed annually and updated as necessary.

Implementation Date:

Completed April 1st, 2026, annual review.

Person Responsible for Implementation:

Caitlyn Vivacqua, Human Resources Clerk.

Recommendation #5:

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

Implementation Plan of Action(s):

The District will implement a documented reconciliation process utilizing reports generated from the building access management system. On a quarterly basis, active employee and non-employee accounts will be reviewed to verify that access remains necessary, appropriate, and properly authorized. The reconciliation will include a review of active badges, duplicate badges, shared badges, expiration dates for temporary access, and access levels. Any discrepancies identified during the review will be corrected promptly and documented.

Implementation Date:

Completed April 1st, 2026, and quarterly thereafter.

Person Responsible for Implementation:

Human Resources Clerk, with oversight by the School Business Administrator.

The District appreciates the recommendations provided by the Office of the State Comptroller and is committed to implementing the corrective actions outlined in this plan to strengthen building access controls and enhance the security of District facilities.

Ashley Brooks
School Business Manager

Allison Goodspeed
Board of Education
Audit Committee Member

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 the non-employee badge request form 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 active accounts list, including 477 accounts, to the full-time employee master list to determine whether all accounts were associated with current District employees. We interviewed District officials and reviewed relevant documentation to determine whether the accounts and badges assigned to non-employee individuals were necessary. For any unnecessary accounts, we inquired as to why they were not deactivated.

- We used our professional judgement to select 42 shared accounts. We included badges with five or more badges assigned to the same third party, for example the same construction company with 15 badges and reviewed the badge access history, including the last time each badge was used.

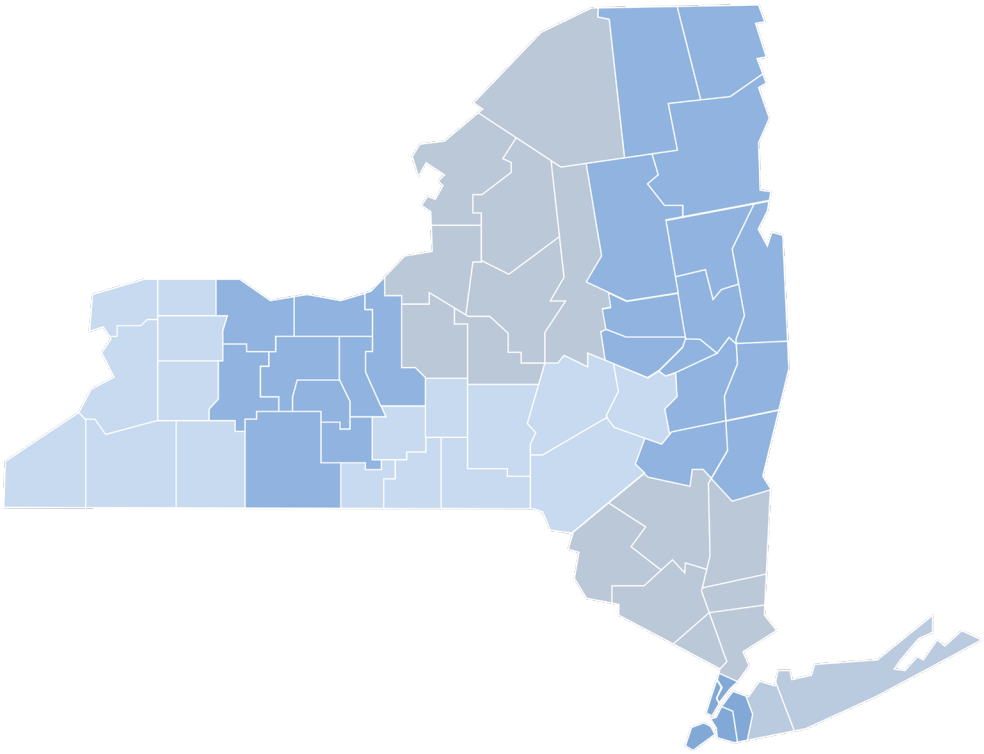
- We reviewed the active accounts list to determine whether any individuals had more than one badge and interviewed District officials to determine why individuals were assigned more than one badge. We identified 12 employees with duplicate badges. We discussed the duplicate badges with the Clerk to determine whether they were necessary or should be deactivated.

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