New York State Comptroller
THOMAS P. DiNAPOLI

Central Square Central School District

Building Access

July 2026 | S9-26-14
Prepared by the Division of Local Government and School Accountability

Table of Contents

Audit Results

Central Square Central School District

Audit Objective

Did Central Square 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 March 12, 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 947 active building access accounts (accounts), including 798 devices issued to current employees and 149 issued to non-employees, of which 45 are shared devices.[1] Each of the District's six 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, the District had active, but unneeded, accounts with assigned badges in the system:

- Nine District employees had duplicate active badges.
- 19 non-employee badges, including 11 former employee badges and one badge which District officials did not know why it was created, were not deactivated when no longer needed.

Furthermore, officials did not establish written policies or procedures or assign responsibilities for managing and monitoring accounts. Although District officials had a process to periodically review active accounts, the process was not effective based on the findings.

The 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.

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 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.

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 March 2026, the District had 947 active accounts associated with 798 badges issued to 789 current employees, and 149 badges issued to 104 individual non-employees including 45 shared badges. We determined:

- Nine current employee accounts had duplicate active badges, and
- 19 of 31 (61 percent) active non-employee accounts we reviewed were unneeded.

<u>Employee Accounts</u> – Of the 789 employees, nine employees were assigned two active badges. We reviewed all nine accounts to determine why the employees were assigned more than one badge and determined that eight of the nine duplicate badges were issued because officials created new accounts and badges but did not deactivate the employees' previous accounts and badges. Specifically:

- Five duplicate accounts and badges were created for employees who changed positions. The personnel department's (Department) personnel assistant (Assistant) explained that when an employee changed positions, she created a new account and issued a new badge, and that the old account and the associated badge remained active until the employee received their new badge, at which point she would deactivate them. However, the Assistant did not deactivate five accounts associated with old badges, even though all five employees received their new badges, one of whom continued to use their older active badge.
- Three duplicate accounts and badges were created to issue replacements for lost or damaged badges. The Assistant could not provide a reasonable explanation why the old badges were not properly deactivated.
- One duplicate badge, assigned to the Assistant, was required only for District operations like printer access but was mistakenly configured for building access.

After our audit inquiry, the Assistant deactivated the eight unneeded duplicate accounts and badges and removed the building access configuration from her duplicate badge.

<u>Non-Employee Accounts</u> – For the individual non-employee badges, we sampled and reviewed 20 of the 104 badges with District officials,[2] and reviewed personnel changes as documented in the November 2025 Board meeting minutes. We determined that 12 active individual non-employee accounts we reviewed were unneeded. Specifically:

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

- Eleven accounts and badges were assigned to former District employees, including one who retired in December 2025, and

- One account and badge was assigned to a BOCES employee who was no longer performing services for the District.

The Assistant told us that five of the 12 unneeded employee accounts and their associated badges remained active because of her brief separation from the District at which time a new staff member was responsible for management of access accounts and did not have written procedures to follow. The Assistant further told us that the remaining seven unneeded employee accounts were not deactivated as a result of her oversight.

Of the 45 shared badges, 34 were assigned to first responders. All 34 badges were created in 2023 or earlier and were never set to expire. In addition, 25 of the first responder badges were never used. District officials did not track or periodically reconcile badges issued to each fire and law enforcement entity to ensure all were still needed. Furthermore, based on the inactivity of these badges, there is a risk that they may be lost or damaged. A lost or damaged badge assigned to a first responder would not only prevent a first responder from accessing the building in an emergency, but because the badges do not expire, a lost badge increases the risk of unauthorized access. We brought this to District administrators' attention, and the Superintendent confirmed that all 34 badges were still needed.

We reviewed the remaining 11 shared badges to determine their necessity and purpose. The Assistant told us that four of the 11 badges were needed for substitute employees, but the remaining seven badges were not needed. Specifically:

- Six shared badges were created to provide building access to substitute employees. Five of these badges were never used and one badge was last used in July 2024. The Assistant confirmed that all six badges were no longer needed.
- One shared badge was created in November 2024 and was never used. District officials did not know why the badge was created but confirmed that it was no longer needed.

When we brought these issues to the District officials' attention, the Assistant deactivated the unneeded 12 non-employee badges and seven shared badges identified in this report.

<u>Account Management and Monitoring Procedures</u> – 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 of revoking access, by deactivating unneeded accounts and collecting badges.

At the time of our fieldwork, building access management was handled by the Assistant. Although the Assistant had a process to periodically review active accounts to determine whether they were needed, this process was not effective based on our audit testing and observation of active, unneeded badges.

During fieldwork, Department officials began to create a written procedure document detailing who is responsible for managing and monitoring building access accounts.

Because District officials did not have building access procedures, access 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 badges as soon as they are no longer needed.

2. Ensure employees do not have duplicate badges.

3. Limit the use of shared badges and ensure every individual (employee, vendor, contractor, or other authorized user) is assigned a unique and individual badge.

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. Periodically monitor and reconcile all badges issued to first responders and confirm with those agencies that all badges are still needed.

Appendix A: Profile, Criteria and Resources

Profile

The District's boundaries include the Towns of Amboy, Constantia, Hastings, Mexico, Palermo, Parish, Schroeppel and West Monroe in Oswego County, the Towns of Cicero and Clay in Onondaga County and the Town of Vienna in Oneida County. The District's buildings are located on campuses in the Town of Hastings (Elementary School building, Middle School building, and High School building); the Town of Constantia (Elementary School building) and the Town of Cicero (Elementary School building).

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 Department, under the direction of the Executive Director of Personnel, is responsible for managing and monitoring accounts. The Assistant activates, modifies and deactivates accounts in the system as well as prints and issues badges to individuals. One other Department staff member and the Executive Director of Planning, Development and Technology also have administrative rights to activate, modify and deactivate accounts in the system if the Assistant 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 their 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.

3 https://www.nysed.gov/sites/default/files/programs/facilities-planning/safeschoolsbydesign-aguidebynysed-april2025.pdf
4 https://www.cisa.gov/sites/default/files/2022-11/k12-school-security-guide-3rd-edition-022022-508.pdf

Device Issuance and Authorization – Devices should only be issued with documented approval based on job role and building assignment, each device should be unique and individually assigned. Each individual should only have one device. Shared devices should be avoided so that all activity can be logged to a specific individual. When shared devices must be used, a process should be established to track these devices. No individual should be issued a device until a background check is completed, if required. Visitors and contractors should sign in at a single point of entry and receive a visible identification or badge. Contractors' access should be limited to approved locations and timeframes.

Device Management − Devices should be immediately deactivated when no longer necessary. Any necessary updates to building access should happen promptly. Lost or stolen devices should immediately be reported to staff responsible for deactivating devices and replacement devices should be reissued only with documentation approving the reissuance. Device inventory should be tracked and periodically reconciled, and unused or returned devices should be secured or destroyed.

Building Access Event Monitoring – Device events should be logged by user, door and timestamp (i.e., device used at door). These logs should be reviewed periodically and/or upon an unauthorized incident. The building access system should generate alerts for after-hours or unauthorized access attempts if possible. Logs should be retained according to the district policies. Periodically reviewing physical access logs can help identify unexpected activity.

Additional Resources

We also used the following publications to inform our criteria. These publications provide school officials with actionable, practical and cost-effective resources, solutions and tools that enhance school building safety and security:

- **NYSED Safe Schools by Design Act: A Guide by NYSED (April 2025)**
  https://www.nysed.gov/sites/default/files/programs/facilities-planning/safeschoolsbydesign-aguidebynysed-april2025.pdf

- **Partner Alliance for Safer Schools (PASS) Safety and Security Guidelines for K-12 Schools (7th Edition, 2025)**
  https://passk12.org/wp-content/uploads/2025/08/PASS_7thEdition-web.pdf

- **K-12 School Security Guide (3rd Edition, 2022)**
  https://www.cisa.gov/sites/default/files/2022-11/k12-school-security-guide-3rd-edition-022022-508.pdf

- **National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations (Revision 5)**
  https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

In addition, local officials can use OSC's website to search for audits, resources, publications and training for officials at: https://www.osc.ny.gov/local-government

Appendix B: Response From District Officials

The content below is a reproduced copy of the original response letter issued by District officials, is reformatted to meet the Americans with Disabilities Act *Web Content Accessibility Guidelines (WCAG)*,[5] and may have included changes to spelling and grammar. The substance of the content was not changed.

CENTRAL SQUARE CENTRAL SCHOOL DISTRICT
44 School Drive
Central Square, NY 13036
P: 315-668-4220 | F: 315-676-4437
www.cssd.org

July 23, 2026

Nicole A. Tomsen, Chief of Municipal Audits
Office of the State Comptroller
Division of Local Government and School Accountability
295 Main Street, Suite 1032
Buffalo, NY 14203-2510

Re: Central Square Central School District – Building Access Audit (Draft Report S9-26-14)

Dear Ms. Tomsen:

The Central Square Central School District expresses its sincere appreciation to the Office of the New York State Comptroller for its thorough evaluation and collaborative approach throughout the building access audit process. District leadership has reviewed the preliminary draft report and concurs with the findings and recommendations aimed at strengthening our overall security architecture. Safeguarding our students, faculty, staff, and visitors is our highest priority. The audit served as a valuable opportunity to identify legacy operational gaps and accelerate comprehensive modernization efforts across our physical security management systems.

Upon notification of the auditors' initial observations in March 2026, District personnel took immediate action to deactivate all unneeded, inactive, or duplicate accounts and badges identified during testing. Furthermore, the District has completed significant infrastructure and policy upgrades designed to address vulnerabilities and establish automated, verifiable controls moving forward.

In response to the specific recommendations outlined on page 5 of the audit report, the District has taken the following actions:

Regarding the timely deactivation of unneeded access, accounts and badges identified during the March 2026 audit were deactivated immediately, completing our initial remediation. To maintain prompt revocations moving forward, the District is implementing a new automated system as of September 2026 that will automatically deactivate badges upon an employee's offboarding from the District's IT system. In June 2026, the District completed an internal review of all active badges, requiring every building principal and department supervisor to review and verify access lists, a process the District plans to conduct annually moving forward.

To address duplicate credentials, unneeded duplicate accounts identified during the March 2026 audit were deactivated immediately. With the full deployment of the District's new badge access system in June 2026, every employee record was audited and verified to ensure no duplicate badges exist within the system. This

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

project is fully completed, and the new platform's configuration prevents duplicate active credentials moving forward.

Concerning shared access, the District successfully completed action in July 2026 by reducing shared badges to a maximum of one per school building. Furthermore, the District established a strict administrative procedure requiring these remaining shared badges to be secured inside the main office and signed out individually when needed.

To establish clear governance and monitoring, the District upgraded its physical door controller hardware boards and server in June 2026, and is currently integrating the software into the District's onboarding and offboarding data synchronization pipeline to ensure credential changes are accurate and timely. Work is currently in progress for August and September 2026, during which the District will formalize written procedures defining explicit roles and responsibilities for employee, non-employee, and shared badges, with a target completion date of September 30, 2026. These procedures will undergo annual administrative reviews.

Finally, in conjunction with these new written procedures, the District is currently developing a confirmation protocol for first responder credentials assigned to local fire and police departments. This reconciliation process will be completed by September 30, 2026, to confirm that all listed badges remain in active use, and the District will continue to conduct these verifications annually.

The District remains committed to maintaining a secure learning environment for our entire school community. We appreciate the recommendations provided by the Office of the State Comptroller, which have helped strengthen our internal control environment. The District looks forward to submitting its formal Corrective Action Plan (CAP) following the final publication of the report.

Sincerely,

Thomas J. Colabufo
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 accounts and badges, including roles and responsibilities of the individuals involved in the process.

- We compared the District's 947 active accounts list to the employee master list to determine whether active accounts were associated with current District employees. Of the 104 active individual accounts that were not assigned to an employee, we used a random number generator and selected 20 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 reviewed Board meeting minutes from November 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 badge.

- We used our professional judgment to select 11 of the 45 shared accounts based on access purpose and inquired with the respective District officials responsible for these badges to determine whether the badges were necessary. For any unnecessary accounts, we inquired as to why they were not deactivated.

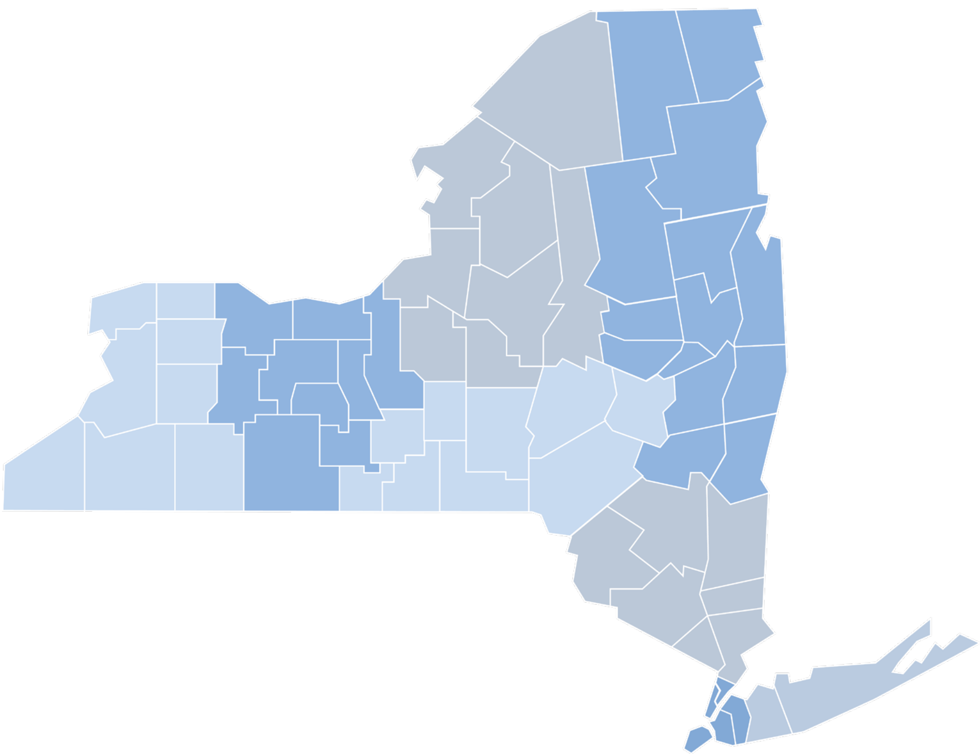
- We reviewed the active building accounts list to determine whether any individuals had more than one account and interviewed District officials to determine why individuals were assigned more than one account. We identified nine employees with a total of 18 duplicate badges and reviewed all duplicate badges. We followed up with District officials to determine why individuals had multiple 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 objectives. Auditors believe that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objective.

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

Questions?

STATEWIDE AUDITS
Nicole A. Tomsen, Chief of Municipal Audits
295 Main Street, Suite 1032 • Buffalo, New York 14203-2510
Tel (716) 847-3647 • Fax (716) 847-3643
Email: Muni-Statewide@osc.ny.gov



Contact

Office of the New York State Comptroller
110 State Street
Albany, New York 12236

(518) 474-4044

www.osc.ny.gov

Prepared by the Division of Local Government and School Accountability

FOLLOW US: osc.ny.gov/subscribe