New York State Comptroller
THOMAS P. DiNAPOLI

Greene Central School District

Building Access

September 2026 | S9-26-3
Prepared by the Division of Local Government and School Accountability

Table of Contents

Audit Results

Greene Central School District

Audit Objective

Did Greene 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 June 3, 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, key cards, 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 350 active building access accounts (accounts) with 359 active devices, including 238 devices issued to current employees and 121 issued to non-employees, of which 67 are shared devices.[1] Each of the District's three school buildings, including the combined Junior/Senior High School, have 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 cards). 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 key cards in the system:

- 18 employees had duplicate active key cards.
- Eight active non-employee key cards were not needed, including three key cards which District officials could not locate.

Although District officials had a process for adding accounts in the system for employees and non-employees, no one periodically reviewed active accounts to determine whether they were needed. Furthermore, these issues occurred because District officials did not develop written policies and procedures that clearly assign roles and define the responsibilities for managing and monitoring accounts or issuing key cards.

This report includes three recommendations that, if implemented, will help District officials improve management and monitoring of building access accounts and key cards. District officials generally agreed with our recommendations and indicated they plan to initiate corrective action. Appendix C includes our comment on an issue District officials raised in their response.

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 D.

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 key cards.

During our fieldwork in May 2026, the District had 359 active key cards, with 238 key cards issued to 220 current employees, and 121 key cards issued to non-employees, including 67 shared key cards. We determined:

- 18 employee accounts had duplicate active key cards.
- Eight active non-employee key cards were not needed, including three key cards which District officials could not locate.

Employee Accounts – Of the 220 current employees, 18 employees (8 percent) had duplicate active devices. The District Clerk (Clerk) and the Superintendent's Secretary (Secretary), who were assigned responsibility for managing and monitoring accounts by the Superintendent, told us that nine of the duplicate key cards were issued as replacements for lost or damaged key cards. The remaining nine key cards were issued to custodial employees, who due to health and safety concerns with using key cards while operating machinery or cleaning, were issued separate key fob devices. Because key cards also serve as employee identification, the custodial employees' key cards were not collected by District officials when the key fobs were issued. However, District officials did not deactivate the key cards' building access function, resulting in duplicate active devices.

We discussed with the Superintendent, Secretary, and Clerk the risk that multiple access devices pose. They agreed to deactivate the key cards' building access function for custodians who also had active key fobs, as well as the key cards that were reported lost or damaged.

Non-Employee Accounts – For the 54 individual non-employee accounts, we determined that five key cards (9 percent) were not disabled when no longer needed. These five key cards included one assigned to an individual with a local emergency services department that District officials could not locate and four assigned to former contractors which were not used in over a year. The 67 shared key cards included two which District officials could not locate: one assigned for emergency services and one for a student lifeguard.

The Clerk and Secretary told us the eight non-employee key cards were not disabled because they assumed that the Head Custodian, who was responsible for requesting access for non-employees, would alert them when a key card was no longer needed and that emergency service providers would keep track of their key cards. However, it was the Clerk's and the Secretary's assigned responsibility for managing and monitoring accounts.

These issues occurred, in part, due to a lack of clear communication of responsibilities between departments, and no documented procedures for managing and monitoring building access, including no regular reconciliation of access accounts and devices using readily available system reports. As a result, the Clerk and Secretary were not aware that employees' lost and damaged keycards were still active, that there were active

unneeded non-employee key cards, and active key cards which they could not locate. As a result of our audit inquiry, the Clerk and Secretary disabled the unneeded accounts.

Account Management and Monitoring Procedures – 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, who is responsible for monitoring active accounts, and the process to revoke access by deactivating unneeded accounts and collecting key cards. At the time of our fieldwork, the process for adding, removing, or modifying access accounts was handled by the Clerk and Secretary who:

- Added accounts for new employees/non-employees to the system including any access restrictions (e.g., days, times and buildings) based on information provided on the onboarding sheet or by the Head Custodian.
- Modified access as requested by building principals.
- Revoked employee access after Board resolution of their separation or notification from the building principal if more immediate.
- Distributed and received access devices, including destroying those that are no longer needed.

The Clerk and Secretary told us that they performed some reviews of accounts, but this was primarily limited to key cards issued to coaches and substitutes including teachers, custodians and food service workers. These key cards were all located and accounted for with each of the building secretaries, interim Head Custodian, and Food Service Manager.

However, no one was periodically reviewing all active accounts and using available system reports to determine whether all active accounts and key cards still needed access. As a result, District officials were unaware that the unneeded key cards were still active. During our fieldwork, we worked with District officials and demonstrated how the system's reports could improve the monitoring and management of building access. When access is not periodically reviewed and revoked, it increases the potential for unauthorized access to District buildings.

Recommendations

District officials should:

1. Continue to deactivate accounts and collect the associated key cards as soon as they are no longer needed.

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

3. 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 portions of the Towns of Coventry, German, Greene, McDonough, Oxford and Smithville in Chenango County and the Towns of Barker and Triangle in Broome County, and the Town of Willet in Cortland County. The District's three buildings are located on campuses in the Town of Greene.

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 and Secretary the responsibility for managing and monitoring accounts. The Clerk and Secretary utilize the system to set up and issue key cards to users, which are then distributed by either of them depending on availability.

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., Information Technology, 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 individual should be issued a device until a background check is completed, if required. Visitors and

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

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)*,[4] and may have included changes to spelling and grammar. The substance of the content was not changed.

Greene Central School District
40 South Canal Street
Greene, New York 13778
Telephone (607) 656-4161
FAX (607) 656-9362

Nicole A. Tomsen
Chief of Municipal Audits, Office of the New York State Comptroller
295 Main Street, Suite 1032
Buffalo, NY 14203-2510

RE: Greene Central School District Building Access Draft Audit Response (Report S9-26-3)

Dear Ms. Tomsen:

On behalf of the Greene Central School District, we appreciate the opportunity to respond to the draft findings and recommendations of the Building Access audit (Report S9-26-3) conducted by your office for the period of July 1, 2024, through November 30, 2025 (as extended to June 3, 2026). The District values the constructive feedback provided by your staff to help strengthen our physical building access controls.

Ensuring the safety of our students, staff, and school community is our highest priority. The District concurs with the recommendations to deactivate unnecessary accounts, collect associated key cards, formalize written management procedures, establish periodic reconciliation processes, and routinely review active accounts. These measures will be fully incorporated into a formal Corrective Action Plan (CAP) to be submitted within the statutory 90-day window following the publication of the final report.

Context and Broader Security Framework

The District views this audit as a valuable management tool to reinforce our commitment to physical security, refine operational workflows, and safeguard our facilities. Modern school security requires balancing evolving access technologies, community facility use, and workforce mobility. While we welcome opportunities to modernize our administrative procedures, the District emphasizes that no security breaches, unauthorized access incidents, or improper entries occurred as a result of the identified accounts. [OSC Comment: See Appendix C, Note 1]

The audit's administrative findings should be viewed alongside the District's multi-layered security infrastructure, which includes:

- Single Points of Entry: Controlled access protocols at each site.
- Surveillance & System Evaluation: Continuous video surveillance coupled with regular door-monitoring upgrades.
- Active Hallway Presence: Staff visibility and dedicated monitoring throughout school buildings.
- School Resource Officers (SROs): Consistent SRO presence on both district campuses.

District Response to Specific Audit Findings

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

Audit Finding 1: District officials did not properly manage and monitor building access accounts and badges.

The District agrees that operational controls can be enhanced. However, we offer the following important context regarding the 18 employees identified with duplicate access credentials:

- Facilities Personnel (9 employees / 50 percent): These individuals were issued both key fobs and access badges to perform operational duties. This redundancy has since been resolved.
- Reported Lost Badges (9 employees / 50 percent): These credentials belonged to staff who had reported their badges lost. System logs confirm that none of these lost badges were ever used to gain entry. All associated accounts were deactivated prior to the conclusion of the on-site audit.
- Non-Employee Accounts: All flagged non-employee accounts were rendered inactive prior to the conclusion of the on-site audit.

System logs confirm zero instances of unneeded credentials being used to gain entry, validating the effectiveness of our physical security and personnel monitoring. However, we do recognize the need for ongoing consistency in administrative practices and protocols, which we will be fully incorporated into our corrective action plan.

Recommendations and Corrective Actions

Recommendation 1: Continue to deactivate accounts and collect associated key cards as soon as they are no longer needed.

District Action: The District has deactivated all unnecessary accounts, collected physical key cards, and disabled all reported lost badges. Clear onboarding and offboarding badge protocols have been established for employees and non-employees. As of June 3, 2026, the District implemented written door-access guidelines specifying role-based access schedules and locations. Continuous monitoring will ensure ongoing compliance.

Recommendation 2: Develop written procedures defining roles and responsibilities for managing and monitoring access accounts and periodically evaluate these procedures.

District Action: The District is formalizing comprehensive administrative procedures for badge management. These procedures will enforce a segregation of duties across roles. The District will also periodically evaluate the access system to ensure inactive badges and/or key fobs are deactivated and collected. Completion Target: November 1, 2026.

Recommendation 3: Develop a reconciliation process utilizing system reports to review active accounts for necessity and appropriateness.

District Action: A bi-annual credential verification protocol has been established requiring the Access Issuer to cross-reference active system credentials against official employee rosters and approved community user lists. Additionally, the District is integrating an automated management system to cross-check credentials against law enforcement databases by September 30, 2026.

Next Steps

The District has already begun reviewing and strengthening its building access procedures to ensure that operational practices are consistently documented, monitored, and supported by appropriate supervisory oversight. An internal audit is scheduled for November 2026 to evaluate the implementation and effectiveness of these new control measures. Combined with our formal Corrective Action Plan, these steps will ensure comprehensive, accountable oversight of our electronic access systems.

We appreciate the audit team's recommendations and view this review as an opportunity to strengthen our building access system to ensure the safety and security of our students, staff, and visitors.

Respectfully,

Lisa-Marie Carter, Ed.D.
Superintendent of Schools

cc: Greene Central School District Board of Education

Appendix C: OSC Comment on the District's Response

Note 1

The audit objective focused on the District's management and monitoring of building access accounts and devices. The audit team assessed the risk of potential security breaches occurring, such as unauthorized access to school buildings, which is significant within the context of this audit objective. Therefore, these audit results cannot be used to conclude there were no security breaches or unauthorized access incidents in the District's operations.

Appendix D: 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, reviewed Board policies and the system's settings to gain an understanding of the District's policies, procedures, practices and system access controls related to managing and monitoring accounts and key cards, including roles and responsibilities of the individuals involved in the process.

- We compared the District's 350 active accounts with 359 active devices list to the master list of employees 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 key cards assigned to employees and non-employee users were necessary. For any unnecessary accounts, we inquired as to why they were not deactivated.

- We selected all 67 shared accounts and reviewed system reports to determine when assigned key cards were last used. We requested that the Clerk and Secretary contact the key card holders, including the two law enforcement agencies, the fire department and local emergency medical services to determine whether the key cards were in their possession and needed. If the key cards were not in their possession, we suggested that the Clerk and Secretary disable the key cards.

- We selected all 54 individual non-employee accounts, reviewed system reports and discussed each account with the Clerk and Secretary to determine when the associated key cards were last used, whether they were accounted for, and whether they were needed.

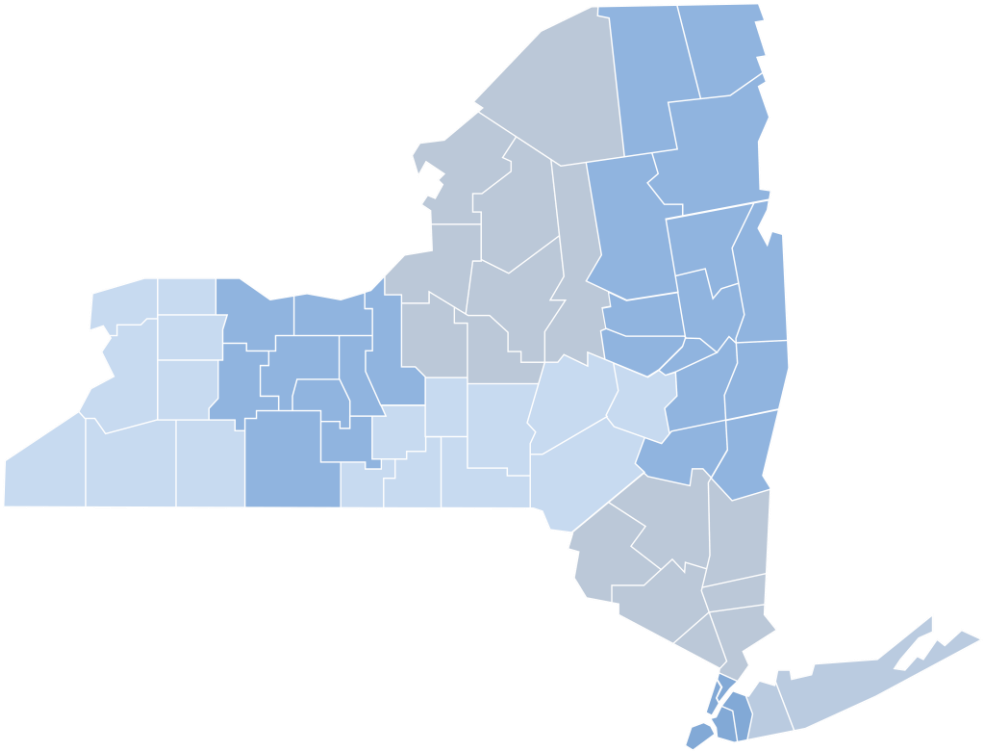
- We reviewed the active accounts list to determine whether any users had more than one account and/or key card. Additionally, we interviewed District officials to determine why employees had multiple active devices, and whether multiple active devices were needed for their duties.

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