

New York State Comptroller
THOMAS P. DiNAPOLI

Groton Central School District

Building Access

August 2026 | S9-26-15

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 key fobs.	3
Recommendations	4
Appendix A: Profile, Criteria and Resources	5
Profile	5
Criteria	5
Additional Resources	6
Appendix B: Response From District Officials	7
Appendix C: Audit Methodology and Standards	9

Audit Results

Groton Central School District

Audit Objective

Did Groton 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 13, 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 179 active building access accounts (accounts), including 159 devices issued to current employees and 20 issued to non-employees, of which eight are shared devices.¹ Each of the District's two 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 (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:

- One employee, the Maintenance Supervisor, had three active key fobs.
- 8 active non-employee key fobs, including two shared key fobs which District officials could not locate, were not needed.

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 fobs.

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 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.

To issue accounts and key fobs for employees, the District used an onboarding form which helped determine which building(s) and level of access was needed. The form required the District Clerk (Clerk) to include the employee’s name, department, and job title and the Maintenance Supervisor to include the key fob number assigned to the employee, the date the key fob was issued, and his authorizing signature.

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 February 2026, the District had 179 active accounts associated with 159 key fobs issued to 157 current employees, and 20 key fobs issued to non-employees, including 12 to individuals and 8 shared key fobs. We determined:

- One current employee, the Maintenance Supervisor, had duplicate key fobs, and
- 40 percent of non-employee accounts were unneeded.

Employee Accounts – Of the 157 current employees, one employee was assigned more than one active key fob, the Maintenance Supervisor, who had three active key fobs. District officials explained that the Maintenance Supervisor required three key fobs due to his role in the event of an emergency. Although District officials were aware that the Maintenance Supervisor had multiple active key fobs and told us why, District officials should recognize that allowing employees to retain multiple active key fobs increases the risk of lost or stolen key fobs which could allow unauthorized entry to District school buildings.

Non-Employee Accounts – Of the 20 non-employee accounts with assigned key fobs, we determined a total of eight non-employee accounts (40 percent) were unneeded, including five assigned to vendors which were never used, one for a project manager which was not used in at least two years and two shared key fobs. For the two shared key fobs, one was assigned to BOCES, and one to a Certified Public Accounting (CPA) firm and were never used, and District officials could not locate them.

When we brought these issues with key fobs to District officials’ attention, the Maintenance Supervisor deactivated all eight unneeded non-employee key fobs. However, these issues occurred, in part, due to a lack of clear communication of responsibilities, and no documented procedures for managing and monitoring building access, including no regular reconciliation of access accounts and devices using readily available system reports. This increased the risk of unauthorized entry to District school buildings.

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 fobs.

At the time of our fieldwork, the process for adding, removing, or modifying access accounts was handled by the Maintenance Supervisor who:

- Added accounts for new employees to the system including any access restrictions (i.e., which days, times and building(s) access was needed for) based on information included on the District's onboarding forms after the Clerk processed their employment paperwork.
- Added accounts for non-employees (e.g., emergency services and BOCES employees).
- Modified access as requested by building leaders (e.g., Superintendent, school building principals).
- Revoked employee access after notification from building leaders or secretaries.

The Maintenance Supervisor told us the elementary and high school secretaries were responsible for collecting key fobs from employees on their last day and that he relied on the secretaries' notification for which key fobs to deactivate and when. He also told us there was no process in place to revoke access for non-employees when it was no longer needed.

Finally, no one was periodically reviewing active accounts and using available system reports to determine whether all active accounts and key fobs were needed. As a result, District officials were unaware that the two unused shared key fobs for the BOCES and CPA firm, which they could not locate, were still active, or that the eight individual non-employee accounts we identified were unneeded. During our fieldwork, we worked with 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. Consider limiting employees to one key fob per individual to lower the risk of loss or misuse.
2. Deactivate accounts and collect the associated key fobs as soon as they are no longer needed.
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 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 parts of the Towns of Locke and Summerhill in Cayuga County, the Town of Homer in Cortland County, and the Towns of Dryden, Groton, and Lansing in Tompkins County. The District's two buildings are located on campuses in the Town of Groton.

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 Maintenance Supervisor the responsibility for managing and monitoring accounts. The Maintenance Supervisor utilizes the system to set up and issue key fobs to users which are then distributed either by him or the Clerk. While other District officials have administrative rights, no one currently serves as a backup to activate, modify and deactivate accounts in the system if the Maintenance Supervisor is unavailable to do so.

Criteria

NYSED's Safe Schools by Design Act guidance² 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 Guide³ 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

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>

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 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 and 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.

Groton Central School District
400 Peru Road
Groton, NY 13037
Phone: 607-898-5301 Fax: 607-898-4647
WWW.GROTONCS.ORG

CORRECTIVE ACTION PLAN AUGUST 12, 2026

Nicole A. Tomsen - Statewide Audits
Chief of Municipal Audits
295 Main Street, Suite 1032
Buffalo, NY 14203-2510

Nicole,

The Groton Central School District has reviewed the recommendations for properly managing and monitoring our building access accounts and devices.

1. The District considered limiting employees to one key fob to lower the risk of loss or misuse. However, the District recognizes the necessity of multiple key fobs being issued given the nature of certain roles and responsibilities of certain positions.
2. The District agrees with the recommendation that deactivating accounts and collecting the associated key fobs as soon as they are no longer needed is a best practice. The District completed the process of disabling associated key fobs throughout the audit time period.
3. The District agrees with the recommendation of developing 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. The District will complete this task prior to beginning of the 2026-27 School Year.
4. The District agrees with the recommendation that District Officials should develop a reconciliation process utilizing system reports, and review active accounts for necessity and appropriateness of access. This process began prior to the audit period, however our frequency of review has shifted to a quarterly review each year.

Sincerely,

Margo Martin

Groton Central School District
District Superintendent

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

School Safety Operating Procedures Building Access Control and Management

Purpose

To establish detailed operational procedures for the implementation, monitoring, and enforcement of building access controls and badge usage, aligned to District administrative regulation and safety expectations.

Scope

These procedures apply to the School Safety Department and supporting personnel responsible for administering and monitoring the Building Access System (BAS).

Operational Procedures

1. Post-Board Personnel Updates

Following each Board of Education meeting, District Clerk will notify Facilities Supervisor with personnel updates including retirements, resignations, terminations, and new hires.

2. Immediate Deactivation Protocol

Access shall be immediately deactivated for any employee not actively present on school grounds, including resignations or administrative reassignment.

3. Usage Monitoring and Audit Cycle

Every four (3) months, the Facilities Department shall audit access credential usage.

4. Lost or Stolen Badges

All reported lost or stolen badges shall be immediately deactivated. Replacement badges will only be issued following verification and documentation.

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 179 active accounts list to the employee 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 fobs assigned to non-employee users were necessary. For any unnecessary accounts, we inquired as to why they were not deactivated.
- We selected all eight shared accounts and reviewed system reports to determine when assigned key fobs were last used. We requested that the Maintenance Supervisor contact the key fob holders, including the police department, fire department, BOCES, and a CPA firm, to determine whether the key fobs were in their possession and needed. If the key fobs were not in their possession, we suggested the Maintenance Supervisor disable the key fobs.
- We selected all 12 individual non-employee accounts, reviewed system reports and discussed each account with the Maintenance Supervisor to determine when the associated key fobs 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 fob. Additionally, we interviewed District officials to determine why the Maintenance Supervisor had three active key fobs. There were no other duplicate accounts or key fobs.

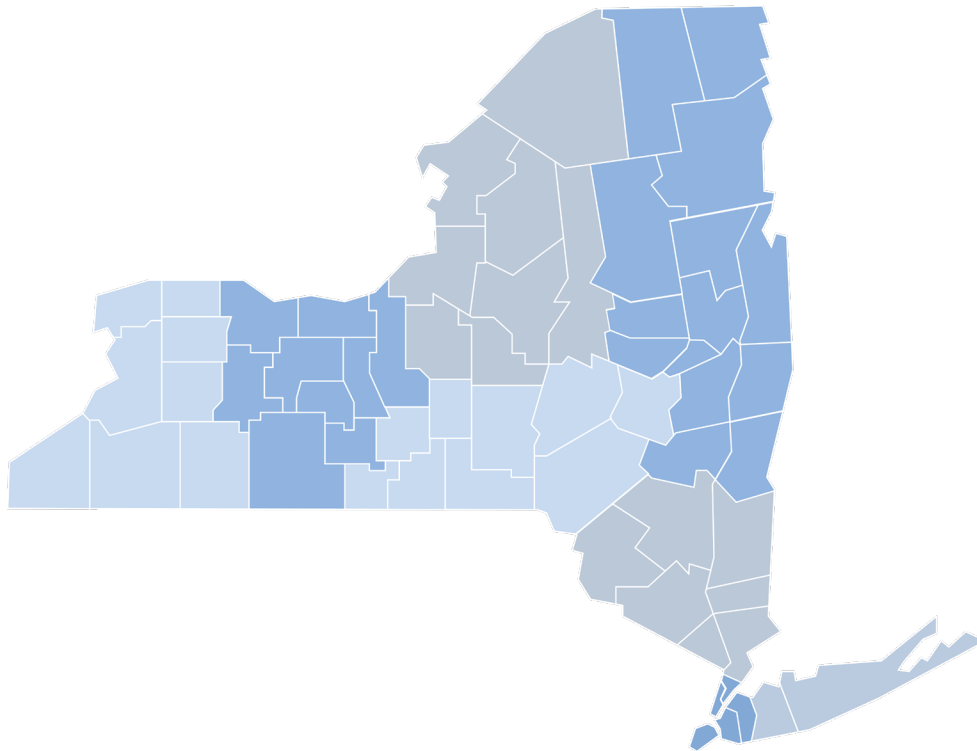
OSC auditors conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that auditors plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. Auditors believe that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objective.

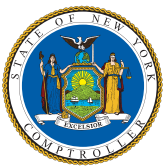
Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or relevant population size and the sample selected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