

New York State Comptroller
THOMAS P. DiNAPOLI

Green Island Union Free School District

Building Access

August 2026 | S9-26-17

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 could improve management and monitoring of building access accounts and badges.	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	8

Audit Results

Green Island Union Free School District

Audit Objective

Did Green Island Union Free 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 10, 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 114 active building access accounts (accounts) associated with 67 devices issued to current employees, and 47 issued to non-employees including 19 shared devices.¹ The District's one school building has one public point of entry. Employees may also use additional secured entry points, which require a device for entry.

Audit Summary

District officials did not identify 12 active, but unneeded, non-employee accounts with active devices (badges). Although District officials had a process for adding accounts in the system for employees and non-employees, and reviewing employee badges in the summer to determine whether they were all needed, no one periodically reviewed non-employee accounts to determine whether they were needed.

District officials also did not develop written policies and procedures that also clearly assign responsibility for managing and monitoring accounts or issuing 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.

This report includes three 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.

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.

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).

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 could improve management and monitoring of building access accounts and badges.

During our fieldwork in February 2026, the District had 114 active accounts associated with 67 badges issued to current employees, and 47 badges issued to non-employees including 19 shared badges.

Non-Employee Accounts – Of the 47 badges assigned to non-employees, we determined 12 were unnecessary. These included:

- Four badges assigned to the contractor who provided and serviced the system,
- Three badges assigned to the school district the District contracted with for food service,
- Two badges with titles in the system that included “returned” or “no longer works here,”
- Two badges assigned to the sheriff department, and
- One badge assigned to a former student teacher.

When we brought these unneeded accounts and badges to District officials’ attention in February 2026, the District Clerk reviewed active accounts and deactivated all 12 of these badges. However, these issues occurred in part due to a lack of documented procedures for monitoring non-employee badges, including no regular reconciliation of access accounts and badges, which raised the risk of unauthorized entry.

Account Management and Monitoring Procedures – District officials created a ‘Building Access Procedures for Employees’ document and an ‘Onboarding and Offboarding checklist,’ which described how to provide and remove badge access from employees, including the employees’ responsibility for reporting lost and stolen badges. However, the District did not have any written procedures clearly defining who is responsible for managing and monitoring accounts. Specifically, District officials did not define who is responsible for monitoring active accounts and badges, and the process to revoke access, by deactivating unneeded access and collecting badges. At the time of our fieldwork, the process for creating access accounts was handled by the District 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.
- Added accounts for non-employees, including volunteers or contractors.
- Printed and issued prenumbered badges to employees and non-employees.

The District Clerk told us she monitored active employee accounts during the summer and was responsible for lost badge deactivation, as well as collecting, deactivating and destroying badges that were no longer needed due to resignation, retirement or termination. She also issued replacement badges if necessary (e.g., lost or damaged badges).

However, there was no process to periodically review non-employee accounts. As a result, account 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 collect the associated badges as soon as they are no longer needed.
2. Develop written procedures that define who is responsible for managing and monitoring accounts including non-employee badges 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 the Town of Green Island (Town) in Albany County. The District's school building is located within the Town.

The District is governed by the elected five-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 District Clerk the responsibility for managing and monitoring building access accounts. The District Clerk utilizes the system to print and issue badges to individuals which are then distributed either by her or the Treasurer in her absence. The Treasurer also has administrative rights to activate, modify and deactivate accounts in the system if the District Clerk 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 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

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>

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.

Green Island UFSD
171 Hudson Avenue
Green Island, NY 12183
P: (518) 273-1422 F: (518) 270-0818
www.greenisland.org

July 29, 2026

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th floor
Albany, NY 12236

Dear Office of the NYS Comptroller:

The Green Island Union Free School District has reviewed the recent draft audit report S9-27-17 regarding Building Access. The school district agrees with the findings and recommendations included within the report. School officials have taken actions to address deficiencies and recommendations included within the NYS Comptroller's draft audit report.

The district looks forward to submitting a Corrective Action Plan within the timeframes required of the NYS Comptroller's Office.

We appreciate the thoroughness with which the audit was conducted and appreciate the recommendations included within the report to strengthen and improve our procedures and documentation related to Building Access.

Sincerely,

Jeffrey P. Simons
Interim Superintendent of Schools

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

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 building access accounts and badges, including roles and responsibilities of the individuals involved in the process.
- We compared the District's 114 active building access accounts list to the employee master list of 66 employees to determine whether all accounts were associated with current District employees. We interviewed District officials and reviewed relevant documentation to determine whether the building access accounts and badges assigned to non-employee individuals were necessary. For any unnecessary accounts, we inquired as to why they were not deactivated.
- We selected all 19 shared accounts and inquired with District officials and reviewed information to determine whether these badges were necessary and how they are maintained.

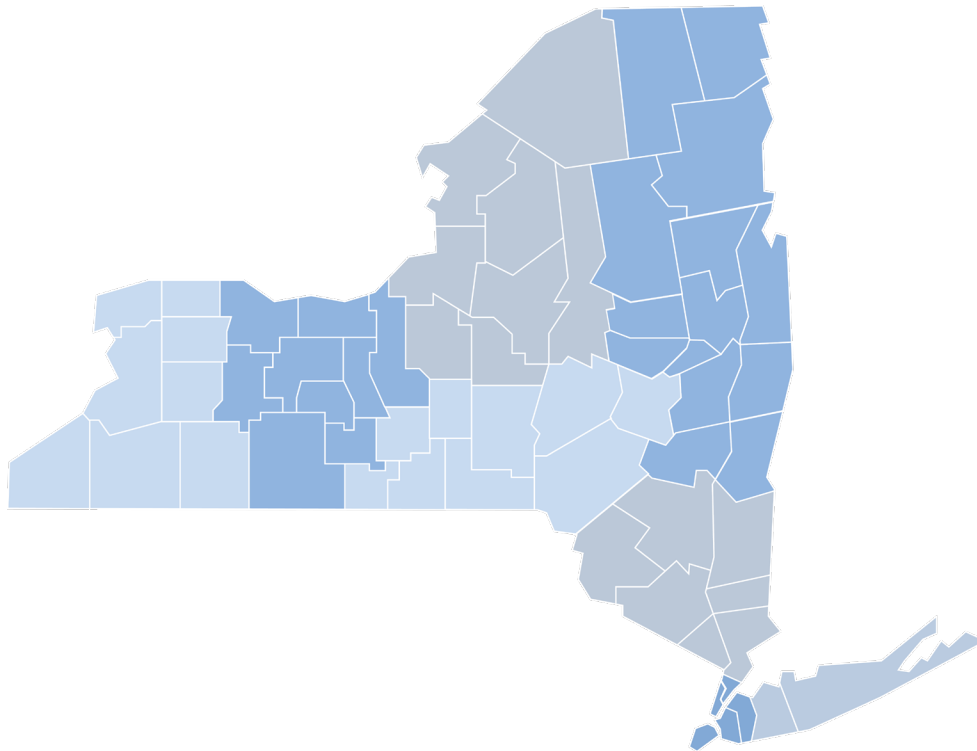
OSC auditors conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that auditors plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on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

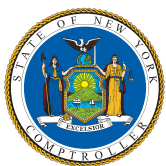
Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or relevant population size and the sample selected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