

New York State Comptroller
THOMAS P. DiNAPOLI

Niskayuna Central School District

Building Access

August 2026 | S9-26-11

Prepared by the Division of Local Government and School Accountability

Table of Contents

Audit Results	1
Building Access: Finding and Recommendations	3
Finding 1 – District officials did not properly manage and monitor building access accounts and badges.	3
Recommendations	5
Appendix A: Profile, Criteria and Resources	6
Profile	6
Criteria	6
Additional Resources	7
Appendix B: Response From District Officials	8
Appendix C: Audit Methodology and Standards	10

Audit Results

Niskayuna Central School District

Audit Objective

Did Niskayuna 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 17, 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 1,140 active building access accounts (accounts), including 997 devices issued to current employees, and 212 issued to non-employees, of which 85 are shared devices.¹ Each of the District's eight school buildings have one public point of entry. Employees may also access the buildings through additional secured entry points, which require a device for entry.

Audit Summary

District officials did not properly manage and monitor building access accounts and devices (badges). As a result, there was a potential risk for unauthorized access to District school buildings, compromising building security and safety for students, teachers, staff and visitors. Specifically, the District had active, but unneeded, accounts with assigned badges in the system:

- 66 individuals, including 61 employees and five non-employees, had duplicate active badges, including two individuals with three active badges.
- 15 shared badges at one school building were not tracked, including one that was not accounted for.

Although District officials had a process for adding accounts in the system, no one periodically reviewed active accounts to determine whether they were needed. Additionally, the monitoring process for shared badges varied by school building and was not effective. These issues occurred because District officials did not develop written policies and procedures for monitoring badges.

This report includes three recommendations that, if implemented, will help District officials improve management and monitoring of building access accounts and badges.

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 your CAP, please refer to our 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.

The District’s Building Badge Access Provisioning standard operating procedure, which was updated during our audit period, described:

- The roles of District officials involved in the building access management process for employees, including information technology (IT) department employees and human resources department employees.
- The processes for adding accounts for new employees, access modification for current employees, lost or stolen badge deactivation and replacement and access revocation.

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 1,140 active accounts associated with 997 badges issued to 934 current employees, and 212 badges issued to non-employees, including 127 to individuals and 85 shared badges. We determined:

- 7 percent of current employee accounts, and 4 percent of individual non-employee accounts had unneeded duplicate active badges,
- 60 percent of the shared badges we reviewed were not tracked, including one badge which District officials could not locate.

Employee Accounts – Of the 934 current employees, 61 employees (7 percent) were assigned two or more active badges, including one employee with three active badges. The Director of Technology (Director) explained that when badges were reported as lost or damaged, and replacements were issued, the original badges were not deactivated as required by District procedures. After our audit inquiry, the Director deactivated all 61 employees’ unneeded duplicate badges and told us the District would improve the process to ensure lost and damaged badges are deactivated immediately once reported.

Non-Employee Accounts – Of the 127 individual non-employees with assigned badges, five individuals (4 percent) were assigned two or more active badges, including a police chief with two active badges and the Director, with three active badges. District officials explained that both the police chief and the Director required two badges each due to their roles; however, the other three individuals’ duplicate badges, as well as the Director’s third badge were not needed and deactivated. As with the duplicate employee badges, these duplicate badges were due to District officials not deactivating lost or damaged badges after issuing replacements.

The 85 active shared badges were used for substitute teachers at the District’s eight school buildings (seven buildings with 10 badges each, and one building with 15 badges), and only provided access to the specific building to which they were assigned. We reviewed the process for monitoring 25 of these badges and their physical availability at two buildings, including the high school (10 badges) and one elementary school (15

badges). We determined the tracking and monitoring of shared substitute teacher badges was handled at the building level, and was not consistent or always effective. Of the 25 shared badges we reviewed, we determined that all 15 at the elementary school (60 percent) were not tracked, including one badge which District officials could not locate.

The elementary school office secretary was responsible for distributing the 15 shared badges to substitute teachers working in the elementary school each day who were expected to return the badge at the end of the day. We reviewed the list of the substitutes working in the building the day of our review to determine whether each substitute teacher had a badge assigned. However, there were no details of which badge the substitute teachers were assigned, nor the time the badges were signed out or returned. Furthermore, although we observed 14 of the 15 substitute badges, District officials could not locate the remaining badge. The Director deactivated this badge in March 2026 when the secretary informed him that it was unaccounted for.

In contrast, the high school main office secretary had custody of and monitored 10 substitute badges that she distributed to substitute teachers working in the high school each day. A sign-in sheet was used to track the substitutes by name, along with the badge number they were assigned, and included the time they checked the badge out and the time the badge was returned. All 10 badges were accounted for.

Account Management and Monitoring Procedures – The District’s procedures were focused on employee badges and included adding accounts for new employees, access modifications for current employees, lost or stolen badge deactivation and replacement, and revocation for terminations.

While at the start of our fieldwork there were no written procedures for non-employees’ badge access and no written procedures outlining who is responsible for monitoring badge accounts, the Building Badge Access Provisioning standard operating procedure was updated during fieldwork to add procedures for non-employees. These procedures included expiration of access and background checks, as well as monitoring procedures to review duplicate badges quarterly and all badge access annually.

The process of adding access accounts was handled by the Director’s secretary (Secretary) 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 (e.g., BOCES employees and contractors).
- Printed and issued prenumbered badges to employees and non-employees.

The Director told us that, as indicated in the District’s written procedures, the Human Resources system synchronizes with the badge access application twice daily, and should automatically revoke access for employees who leave the District. We determined this process for revoking access was working effectively by reviewing recent Board meeting minutes and confirming that badge access was deactivated for individuals who left the District’s employment.

However, no one was periodically reviewing all active accounts to determine whether they were needed or accounted for. As a result, account updates were not always made in a timely manner to deactivate duplicate or unaccounted for badges, such as those we identified. The Director told us that because of our audit, he was aware he needed to perform a review of duplicate badges and update the process going forward to ensure lost and broken badges are deactivated. As previously stated, the Director deactivated all duplicate badges we identified during our fieldwork.

These issues occurred, in part, due to a lack of procedures for monitoring building access, including no regular reconciliation of access accounts and devices, and lack of standardized procedures to account for the substitute badges across the District’s eight schools, which raised the risk of unauthorized entry to District school buildings.

Recommendations

District officials should:

1. Ensure individuals do not have duplicate active badges.
2. Track and monitor the shared badges at all schools to ensure they are accounted for and deactivated if unaccounted for.
3. Annually reconcile badge access accounts, as included in the updated procedures, utilizing system reports to review and remove any duplicate or unneeded badges.

Appendix A: Profile, Criteria and Resources

Profile

The District's boundaries include the Town of Colonie in Albany County, the Town of Clifton Park in Saratoga County and the Towns of Glenville and Niskayuna in Schenectady County. The District's eight school buildings are located on campuses in the Towns of Niskayuna (Birchwood Elementary School, Craig Elementary School, Hillside Elementary School, Rosendale Elementary School, Iroquois Middle School, Van Antwerp Middle School, and Niskayuna High School) and Clifton Park (Glenclyff Elementary School).

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 Director the responsibility for managing and monitoring building access accounts. The Director's Secretary utilizes the system to print and issue badges, which she distributes to individuals. The Director and three other IT department staff members also have administrative rights to activate, modify and deactivate accounts in the system if the Secretary 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.

² <https://www.nysed.gov/sites/default/files/programs/facilities-planning/safeschoolsbydesign-aquidebynysed-april2025.pdf>

³ <https://www.cisa.gov/sites/default/files/2022-11/k12-school-security-guide-3rd-edition-022022-508.pdf>

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

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

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

Niskayuna Central School District
1430 Balltown Road
Niskayuna, NY 12309
(518) 377-4666 phone (518) 377-4074 fax
www.niskayunaschools.org

July 20, 2026

VIA EMAIL (Muni-Statewide@osc.ny.gov)

Nicole Tomsen
Chief of Municipal Audits, Statewide Audits
Division of Local Government and School Accountability

RE: Niskayuna Central School District- Building Access Audit (S9-26-11)

Dear Ms. Tomsen:

The Niskayuna Central School District ("District") acknowledges receipt of the State Comptroller's Preliminary Draft Audit Findings regarding building access. Thank you for providing the District with the opportunity to comment on the same. District officials have reviewed the Preliminary Draft, and generally agree with the findings and recommendations contained therein, as explained more fully below.

Ensuring the safety of the District's students, staff and school community is our highest priority. We appreciate the insights and guidance provided in this audit, which has provided the District with an opportunity to evaluate and strengthen its building access management practices. As noted in the Draft Audit Report, the District had established procedures governing employee and non-employee building access. Nevertheless, the audit review identified certain areas where the District's procedures could be further strengthened. During the course of the audit, and since that time, District officials have already implemented various changes and enhanced District procedures to address the identified areas.

Specifically, with respect to the issuance of duplicate and/or replacement building access cards, the District's Director of Technology immediately took steps to deactivate the unneeded duplicate badges of the small percentage of employees identified as having duplicates. Further, the Director has developed procedures to help ensure that lost and damaged badges are deactivated immediately once reported. With respect to non-employees, the District's standard operating procedures were updated during the course of the audit to address these individuals, including the addition of procedures for expiration of access and background checks, as well as monitoring procedures to review duplicate badges quarterly and all badge access annually.

As noted in the Draft Report, the District had in place a system at the High School which ensured an accurate accounting of badges issued to substitutes on a daily basis, including custody and monitoring of the badges by an assigned person, and the use of a sign-in sheet that provided for the tracking of badges by name, number, time in and time out. District administration will ensure that this process will be communicated across the District and uniformly implemented at all school buildings throughout the District beginning with the upcoming school year.

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

Finally, the Director of Technology and District Administration will review badge access parameters on an annual basis. This review will include a rigorous reconciliation process of all badge access accounts, as per the District's updated procedures, to ensure all accounts are actively reviewed, regularly monitored, and updated as needed.

The District appreciates the recommendations provided in the Draft Report and believes the actions already completed, and those that will be implemented at the beginning of the 2026-2027 school year, will further strengthen its existing procedures in support of maintaining a safe and secure learning environment.

Very truly yours,

Carl J. Mummenthey
Superintendent of Schools
cmummenthey@niskyschools.org

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 our 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 procedures 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 active badge access accounts list, which included 1,140 accounts, to the employee master list to determine whether accounts were associated with current District employees. We interviewed District officials and reviewed relevant documentation to determine whether the badge access accounts and badges assigned to non-employees were necessary. For any unnecessary accounts, we inquired as to why they were not deactivated.
- We used our professional judgment to select all 10 shared badges in the high school and all 15 shared badges in an elementary school and inquired with the respective District officials responsible for these badges to determine whether they were in their possession. If the badges were not in their possession, we inquired to determine why and attempted to locate the badges.
- We reviewed the active badges accounts list to determine whether any individuals had more than one account and badge and interviewed District officials to determine why individuals were assigned more than one account. We identified 66 individuals with a total of 134 badges (61 employees and five non-employees). We followed up with the Director to determine why they had multiple badges.

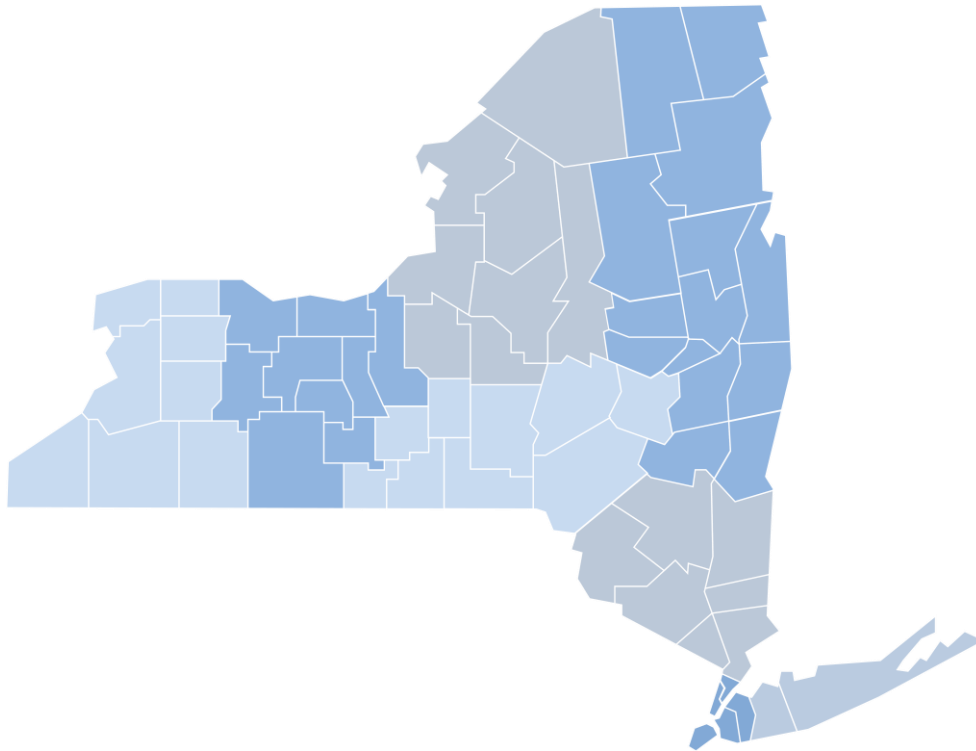
OSC auditors conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that auditors plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on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

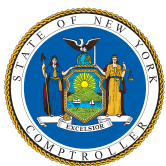
Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or relevant population size and the sample selected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



FOLLOW US: osc.ny.gov/subscribe