New York State Comptroller
THOMAS P. DiNAPOLI

New York Mills Union Free School District

Building Access

July 2026 | Report S9-26-18
Prepared by the Division of Local Government and School Accountability

Table of Contents

Audit Results

New York Mills Union Free School District

Audit Objective

Did New York Mills 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 April 14, 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 117 active building access accounts (accounts), including 74 devices issued to current employees and 43 issued to non-employees, of which two are shared devices.[1] The District also had 177 inactive non-employee accounts and devices for first responders. 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 properly managed and monitored the District's 117 active building access accounts and devices (badges). Except for minor discrepancies, District officials:

- Periodically reviewed active accounts and removed those that were no longer needed in a timely manner,
- Clearly assigned responsibilities for managing and monitoring active employee accounts, and
- Developed written procedures for adding accounts in the system for employees, issuing badges and monitoring the accounts and associated badges.

However, District officials did not ensure that an additional 177 non-employee badges issued for first responders remained active. Although District officials reactivated all 177 badges when we brought this issue to their attention, there was a potential risk that first responders could not access District school buildings when needed, compromising building security and safety for students, teachers, staff and visitors.

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 report includes two 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.

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.

The District contracts with the Oneida-Herkimer-Madison (OHM) BOCES for information technology (IT)-related services provided by the Mohawk Regional Information Center (MORIC). MORIC assigned an Educational Technology Leader (ETL) to manage the District’s building access under the direction of the Superintendent.

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 properly managed and monitored active building access accounts and badges.

During our fieldwork in April 2026, the District had 117 active accounts associated with 74 badges issued to current employees, and 43 badges issued to non-employees including 41 issued to individuals and two shared badges. We determined:

- Except for minor discrepancies, which we discussed with District officials, all 117 active access accounts and badges were adequately managed and monitored.
- An additional 177 non-employee badges issued to first responders were inadvertently deactivated.

<u>Active Accounts and Badges</u> – District officials developed and established written procedures for physical access control, onboarding and offboarding. The procedures collectively define roles, responsibilities and processes for creating, managing, monitoring and revoking accounts and badges for employees. Based on our review of accounts and badges, we determined that District officials adequately followed these procedures. In addition, MORIC staff and the Superintendent periodically reviewed active accounts to determine whether the accounts were needed. As a result, account updates were made to limit the potential for unauthorized access to District buildings.

<u>Inactive Accounts and Badges</u> – The District’s written procedures did not include how District officials should manage and monitor accounts and badges for non-employees. Also, the most recent review of accounts between MORIC staff and the Superintendent only included active accounts. While the ETL told us that she monitored non-employee active accounts and that she followed the same process for employees with non-employees, we identified that the District’s system settings automatically deactivated a total of 177 first responder badges after 90 days of inactivity. All 177 of these badges should have remained active in case of emergency.

The ETL and Superintendent told us that they did not know the inactivity setting was in place and that it should not be applied to first responders. When we brought this issue to their attention, the ETL reactivated all 177 badges, which we confirmed. This automated control, without adequate application and monitoring, and the resulting deactivated badges may have impaired emergency responders’ ability to access District buildings if needed.

Recommendations

District officials should:

1. Develop written procedures that define who is responsible for managing and monitoring non-employee accounts and badges and periodically evaluate and adjust these procedures to ensure all processes are working as intended.

2. Periodically monitor and reconcile all badges issued to first responders and ensure required badges are active.

Appendix A: Profile, Criteria and Resources

Profile

The District's boundaries include the Towns of New Hartford and Whitestown in Oneida County. The District's two school buildings are located on a campus in the Town of New Hartford.

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 District obtains IT services from the OHM BOCES, which provides support through MORIC, including the oversight of building access account administration. The ETL, a MORIC employee, is responsible for managing and monitoring building access accounts, and utilizes the system to issue badges to users which she or department heads distribute to individuals. The Superintendent and building principals also have administrative rights to activate, modify and deactivate accounts in the system if the ETL is unavailable to do so.

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.

<u>Policies and Procedures</u> – Schools should develop and implement physical security and access control policies and procedures with roles and responsibilities defined and assigned across their organizational entities (e.g., IT, Human Resources, administration, facilities, etc.). Policies and procedures should be established to manage, monitor and revoke building access devices and other access credentials as necessary. The policies and procedures should be periodically reviewed and updated to reflect the current and approved access controls implemented within the system and organization.

<u>Building Access/Entry</u> – 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.

<u>Building Access Account Management</u> – 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.

<u>Device Issuance and Authorization</u> – 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 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.

NY Mills Union Free School District
1 Marauder Boulevard
New York Mills, NY 13417

July 20, 2026
Office of the New York State Comptroller (OSC)
Division of Local Government and School Accountability
110 State Street
Albany, New York 12236

Via Email: Muni-Statewide@osc.ny.gov
Attention: Nicole A. Tomsen, Chief of Municipal Audits
Subject: Response– Building Access Audit (Report S9-26-18)

Dear Chief of Municipal Audits and OSC Audit Team:

The New York Mills Union Free School District appreciates the professionalism of the Office of the State Comptroller throughout the audit process. The District shares the Comptroller's commitment to maintaining a safe and secure learning environment for our students, staff, and visitors and values the opportunity to review our practices and strengthen our internal controls.

Overall, the audit confirms that District officials have established and effectively implemented procedures for managing and monitoring active building access accounts and badges. As noted in the report, the District properly managed its 117 active building access accounts and demonstrated sound practices for issuing, monitoring, and removing employee access credentials.

The District acknowledges the audit's recommendations regarding the management of non-employee building access credentials, specifically those assigned to first responders. During the audit process, District officials worked collaboratively with and immediately addressed the issue identified by the auditors. Upon notification, all first responder badges were promptly reactivated, eliminating the potential access concern identified during the review.

The District provides the following responses to the audit recommendations:

Recommendation 1

Develop written procedures that define who is responsible for managing and monitoring non-employee accounts and badges and periodically evaluate and adjust these procedures to ensure all processes are working as intended.

District Response:

The District agrees with this recommendation and has already begun implementing additional procedures. Existing written procedures governing employee access accounts will be expanded to include non-employee accounts, including those issued to first responders, contractors, vendors, and other authorized users. The

---

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

revised procedures will clearly define roles and responsibilities for the Superintendent, District administration, and staff responsible for system administration.

The District will also establish a documented annual review process to verify that all non-employee accounts remain appropriate and necessary and that system settings continue to align with District expectations and operational needs.

Recommendation 2

Periodically monitor and reconcile all badges issued to first responders and ensure required badges are active.

District Response:

The District agrees with this recommendation. Following notification during the audit, all first responder badges were immediately reactivated. Going forward, District officials will conduct periodic reconciliations of all first responder credentials in collaboration with local emergency response agencies to verify that badges remain active, accurate, and available for emergency access when needed.

Additionally, the District will incorporate verification of system inactivity settings into its regular review process to ensure that automated system functions do not inadvertently deactivate credentials required for emergency response.

Corrective Action Plan (CAP)

The District will implement the following actions:

- Revise existing building access procedures to specifically address non-employee access accounts and badges.
- Clearly identify administrative responsibilities for authorizing, monitoring, and reviewing non-employee credentials.
- Establish periodic reconciliation of all first responder access credentials with local emergency agencies.
- Conduct routine reviews of system settings, including inactivity parameters, in collaboration with MORIC to ensure they remain consistent with District policy and operational needs.
- Continue periodic reviews of all active building access accounts as part of the District's ongoing internal control and security practices.

The District expects these procedural revisions and monitoring practices to be fully implemented during the 2026–2027 school year.

The New York Mills Union Free School District appreciates the recommendations provided through this audit. While the audit recognized that the District has appropriate controls in place for managing active building access accounts, the District is committed to continuous improvement and will implement these additional measures to further strengthen its building security program and emergency preparedness.

Sincerely,

Michele D. LaGase
Superintendent of Schools

Appendix C: Audit Methodology and Standards

OSC auditors obtained an understanding of internal controls that were deemed significant within the context of the audit objective and assessed those controls. Information related to the scope of the work on internal controls, as well as the work performed in the audit procedures to achieve the audit objective and obtain valid audit evidence, included the following:

- We interviewed District officials and reviewed Board policies to gain an understanding of the District's policies, procedures and practices related to managing and monitoring accounts and badges, including roles and responsibilities of the individuals involved in the process.

- We compared the District's active accounts list, including 117 active accounts, 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 badges assigned to non-employee users were necessary. We also reviewed the additional inactive 177 first responder accounts and badges that were subsequently reactivated during fieldwork.

- We selected two shared badges 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 accounts list to determine whether any users had more than one account and badge.

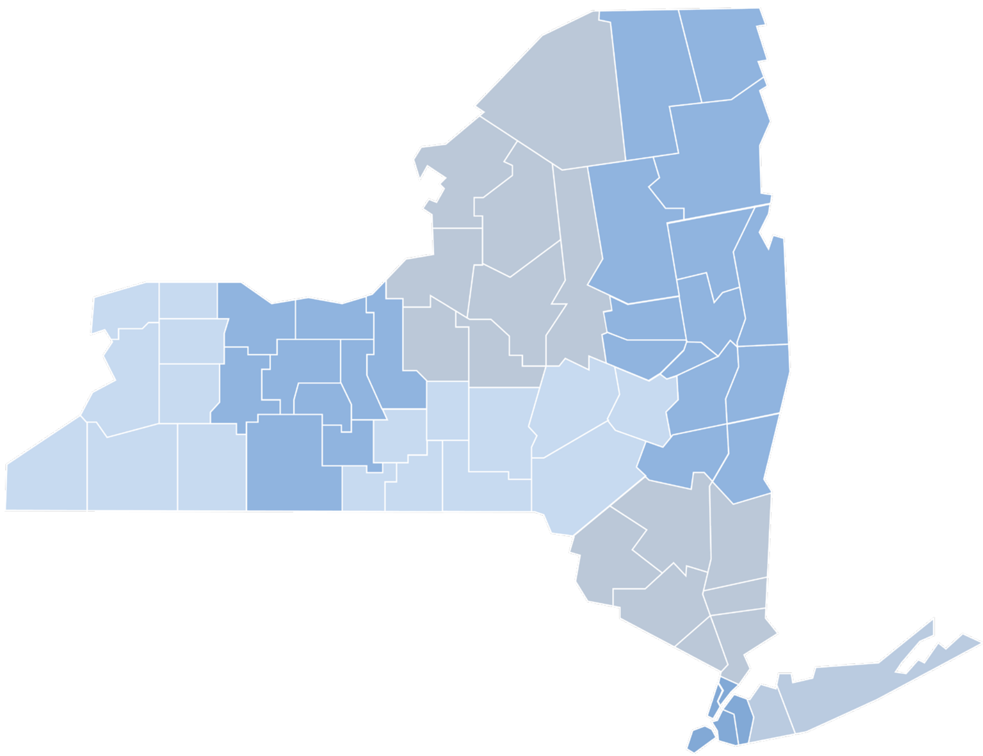
OSC auditors conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that auditors plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on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

https://www.osc.ny.gov

Prepared by the Division of Local Government and School Accountability