New York State Comptroller
THOMAS P. DiNAPOLI

Onondaga Cortland Madison Board of Cooperative Educational Services

Building Access

August 2026 | S9-26-2
Prepared by the Division of Local Government and School Accountability

Table of Contents

Audit Results

Onondaga Cortland Madison Board of Cooperative Educational Services

Audit Objective

Did Onondaga Cortland Madison Board of Cooperative Educational Services (OCM BOCES) officials properly manage and monitor building access accounts and devices?

Audit Period

July 1, 2024 – November 30, 2025

We extended our audit period to January 21, 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.

OCM BOCES utilizes a building access management system (system) with 1,308 active building access accounts (accounts), including 846 devices issued to current employees and 443 issued to non-employees, of which 251 are shared devices.[1] Each of the OCM BOCES' 12 buildings 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

OCM BOCES 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 OCM BOCES school buildings, compromising building security and safety for students, teachers, staff and visitors. Specifically, of the accounts we reviewed, OCM BOCES had active, but unneeded, accounts with assigned badges in the system:

- 141 active individual non-employee accounts and badges were not needed. One of these badges was assigned to an individual who OCM BOCES officials did not recognize and were unable to identify why this individual had access.

- 86 shared accounts and badges were not needed and should be deactivated. OCM BOCES officials could not locate 11 of these badges.

In addition, OCM BOCES officials did not independently verify the background checks for 14 individual non-employees who had direct contact with students, such as third-party service providers, to whom they provided 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).

Although OCM BOCES officials had a written procedure for adding accounts in the system for employees and non-employees, there was no process to promptly disable or delete accounts when no longer needed. Furthermore, these issues occurred because no one periodically reviewed active accounts to determine whether they were needed.

The report includes four recommendations that, if implemented, will help OCM BOCES officials improve management and monitoring of building access accounts and badges. OCM BOCES officials generally agreed with our recommendations and their response is included in Appendix B. Appendix C includes our comments about issues raised in OCM BOCES' response.

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 New York State General Municipal Law (GML). The audit's methodology and standards are included in Appendix D.

The OCM BOCES 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 our office 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 the OSC brochure, *Responding to an OSC Audit Report*, which was provided with the draft audit report. The CAP should be posted on the OCM BOCES'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 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 OSC makes available to local officials that can help them improve operations, are included in Appendix A.

Finding 1 – OCM BOCES officials did not properly manage and monitor building access accounts and badges.

During our fieldwork in January 2026, OCM BOCES had 1,308 active accounts associated with 846 badges issued to current employees, and 443 badges issued to non-employees including 192 issued to individuals and 251 shared badges. We determined:

- 73 percent of active individual non-employee accounts, and 34 percent of active shared accounts were unneeded,
- 13 percent of the active shared badges officials could not locate.
- Officials did not independently verify the background checks for individual non-employees.

<u>Non-Employee Accounts</u> – Of the 192 individual non-employee accounts, we determined 141 active individual non-employee accounts (73 percent) were no longer needed. Specifically:

- 136 accounts were likely assigned to former employees based on records of access activity or other information available to us during our fieldwork. Each of these accounts was tied to a specific individual by name and contained a unique employee identification number (ID). However, the names and/or the IDs did not match those listed on the current employee master list. Based on access activity records, 87 of the 136 accounts' badges were either never used or were last used in 2023 or prior, with some badges last used in 2014.
- Four accounts we reviewed with officials[2] were assigned to former employees who separated from OCM BOCES as early as 2012, and
- One account was assigned to an individual who officials did not recognize and they were unable to identify why this individual had access.

The 251 active shared badges included 227 badges for summer school substitute employees and 24 for various purposes, including contractors and other substitute employees. We selected a sample of 15 active shared badges and expanded our review to include all 251. We determined that 86 of the 251 badges (34 percent) were likely no longer needed based on the records of access activity, and officials should have deactivated them; 30 of the 86 accounts had no record of use since their creation, and the remaining 56 accounts were last used in 2023 or earlier.

2 See Appendix D for details of our sampling and testing methodology.

The Director of Facilities (Director) told us that 75 of the 86 accounts were for summer school substitutes, and that they remained active in case the OCM BOCES needed extra badges. However, officials could not explain why the remaining 11 were still active. While we observed that the badges for the summer school substitute employees were stored in a secure location when not in use, officials were unable to locate the other 11 shared badges.

When we brought these issues to officials' attention, the Director told us that his department was reviewing and deactivating unnecessary accounts and badges. However, these issues occurred, in part, due to a lack of clearly documented procedures for promptly deactivating or deleting accounts when no longer needed. Additionally, there was no regular reconciliation of active accounts and badges, which increased the risk of unauthorized entry.

<u>Non-Employee Background Checks</u> – Officials provided accounts and badges to individual non-employees who had direct contact with students, such as third-party service providers. While these contracted individuals are generally required to undergo fingerprinting for background checks, officials stated that they relied on the assertation of the third-party service providers, rather than by independently verifying these individuals. Although none of the 14 individuals identified by BOCES officials as contractual service providers with direct student contact appeared on New York State Division of Criminal Justice Services sex offender registry, relying solely on third-party vendors to verify their employees creates a risk that individuals who should not be in direct contact with students could gain access to OCM BOCES facilities. Further, OCM BOCES already uses technology to screen visitors entering buildings where students are present, providing assurance that individuals do not appear on prohibited registries. Officials could leverage this existing technology to ensure that non-employees are appropriately vetted before issuing these individuals badges.

<u>Account Management and Monitoring Procedures</u> – Although officials established a written procedure for adding new employee accounts to the system and distributing badges, there were no written procedures that defined the process to describe the roles of individual(s) responsible for managing accounts and devices, add, change and deactivate access for non-employees, revoke access by deactivating unneeded accounts and collecting badges, and monitor active accounts. Furthermore, no one was periodically reviewing active accounts to determine whether all accounts were needed.

The Director told us that his department conducted a one-time review of the active accounts in 2024 and identified individuals whose access to OCM BOCES buildings was no longer needed. However, we noted that this review did not identify the issues found during our fieldwork. He also explained that a Facilities department employee would refer to the personnel agenda listed on monthly Board meeting minutes in updating and managing access accounts, but this practice was no longer in place since this employee was on extended leave. The Assistant Director of Facilities (Assistant Director) temporarily assumed the employee's responsibilities of adding and removing accounts and badges while the employee was on leave, but told us that these reviews were not completed due to competing priorities and lack of resources. As a result, account updates were not always made in a timely manner and there was a potential for unauthorized access to OCM BOCES buildings due to untimely account deactivation.

Recommendations

OCM BOCES officials should:

1. Deactivate accounts and collect the associated badges as soon as they are no longer needed.

2. Consider verifying background checks, utilizing existing technology, for non-employee individuals with direct student contact prior to authorizing their building access account and badges for access to OCM BOCES buildings.

3. Develop written procedures that define who is responsible for managing and monitoring accounts including shared badges 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

OCM BOCES is composed of 23 component school districts. OCM BOCES provides instructional and support programs and services at 12 locations within the counties of Onondaga, Cortland and Madison.

OCM BOCES is governed by its 11-member Board, elected by the board members of the component school districts' boards of education. The Board is responsible for managing and controlling the OCM BOCES' financial and educational affairs. The District Superintendent is responsible, along with other administrative staff, for managing the OCM BOCES' day-to-day operations under the Board's direction.

An employee within the Facilities Department is responsible for managing and monitoring accounts by utilizing the system and printing and issuing badges to individuals which are then distributed by the department heads. The Director and the Assistant Director also have administrative rights to activate, modify and deactivate accounts in the system if this employee is unavailable to do so.

Criteria

NYSED's Safe Schools by Design Act guidance[3] 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[4] 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 (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.

<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

3 https://www.nysed.gov/sites/default/files/programs/facilities-planning/safeschoolsbydesign-aguidebynysed-april2025.pdf
4 https://www.cisa.gov/sites/default/files/2022-11/k12-school-security-guide-3rd-edition-022022-508.pdf

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 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 OCM BOCES Officials

The content below is a reproduced copy of the original response letter issued by OCM BOCES officials, is reformatted to meet the Americans with Disabilities Act *Web Content Accessibility Guidelines (WCAG)*,[5] and may have included changes to spelling and grammar. The substance of the content was not changed.

OCM BOCES
110 Elwood Davis Road
Liverpool NY 13088
www.ocmboces.org

July 27, 2026

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

OCM BOCES Building Access Draft Audit Response (Report S9-26-2)

Dear Ms. Tomsen,

On behalf of Onondaga-Cortland-Madison Board of Cooperative Educational Services (OCM BOCES), we appreciate the opportunity to respond to the draft findings and recommendations of the Building Access audit (Report S9-26-2) conducted by your office for the period of July 1, 2024, through November 30, 2025 (as extended to January 21, 2026).

OCM BOCES accepts the findings and agrees with the recommendations. We view the audit process as a valuable management tool to enhance our physical security infrastructure, refine our internal workflows, and safeguard our facilities for students, staff, and visitors. We recognize that despite the Comptroller's findings, no security breaches or unauthorized access incidents occurred as a result of the identified accounts [OSC Comment: See Appendix C, Note 1].

Coincidentally, prior to the commencement of this audit, OCM BOCES had already identified several areas for improvement. In the summer and fall of 2025, OCM BOCES proactively began working on implementing a formal, comprehensive off-boarding process designed to ensure the immediate termination of badge access and the physical collection of employee badges upon separation. We have already deactivated the unnecessary accounts identified during your fieldwork and are appreciative of the insight provided by your audit team.

Below are responses and clarifications regarding the findings, along with the corrective steps OCM BOCES has already initiated.

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

Management of Non- Employee and Shared Accounts

- As a large regional shared service agency, OCM BOCES experiences high seasonal fluctuations in staffing, substitute personnel, summer school staffing and third-party contractors. To ensure continuous operations and immediate badge availability, a controlled pool of shared devices was maintained[OSC Comment: See Appendix C, Note 2].

- OCM BOCES has now instituted expiration dates on all temporary and shared badge profiles to prevent accounts from remaining active past their intended utility.

Non-Employee Background Checks

The report highlights individual non-employee third-party service providers whose background checks were not independently verified by BOCES.

- As stated above, moving forward, OCM BOCES has already begun implementing a written procedure, in accordance with applicable law, requiring direct fingerprinting verification for OCM BOCES regular onsite vendor employees as part of our standard contracting process before any badge access is authorized.

- For all other non-employee situations, OCM BOCES is developing procedures to expand the deployment of our Raptor Visitor Management System to ensure real-time, independent registry screening.

Account Management and Monitoring Procedures

OCM BOCES recognizes the need for formalizing our internal checks and balances to prevent gaps in account monitoring, particularly during personnel leaves. We have formalized a reconciliation process which OCM BOCES will share in further detail in the subsequent formal Corrective Action Plan.

We are committed to continuously improving our security protocols, which we have already begun. We are fully incorporating all four of the Comptroller's recommendations into a formal Corrective Action Plan, which will be submitted within the statutory 90-day window following the publication of the final report.

We want to thank the State Comptroller’s field staff for their professionalism, positive/encouraging interactions, and constructive feedback throughout this audit process.

Respectfully,

Matthew L. Cook, Ed.D.
District Superintendent

Appendix C: OSC Comments on OCM BOCES' Response

Note 1

The audit objective focused on OCM BOCES' 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 OCM BOCES' operations.

Note 2

During our fieldwork, we identified that 227 of 251 active shared badges were for summer school substitute employees, and were stored in a secure location when not in use. However, we did not observe, and therefore cannot conclude, that the remaining 24 badges were also maintained in a controlled pool. As indicated in Finding 1, officials were unable to locate 11 of the remaining 24 shared badges.

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 our 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 OCM BOCES officials and reviewed Board policies to gain an understanding of the OCM BOCES' 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 OCM BOCES' 1,308 accounts list to the employee master list of 1,148 employees to determine whether accounts existed that were not associated with current OCM BOCES employees. We interviewed OCM BOCES officials and reviewed relevant documentation to determine whether the accounts and badges assigned to 192 non-employee individuals were necessary. For any unnecessary accounts, we inquired as to why they were not deactivated. For any necessary accounts, we inquired as to the purpose of the accounts and identification of the non-employee individuals who were assigned the accounts.

- We interviewed OCM BOCES officials for the general vetting process for non-employee individuals and checked the names of 14 non-employee individuals whom OCM BOCES officials identified as a service provider with student contact against the New York State Division of Criminal Justice Service's sex offender registry.

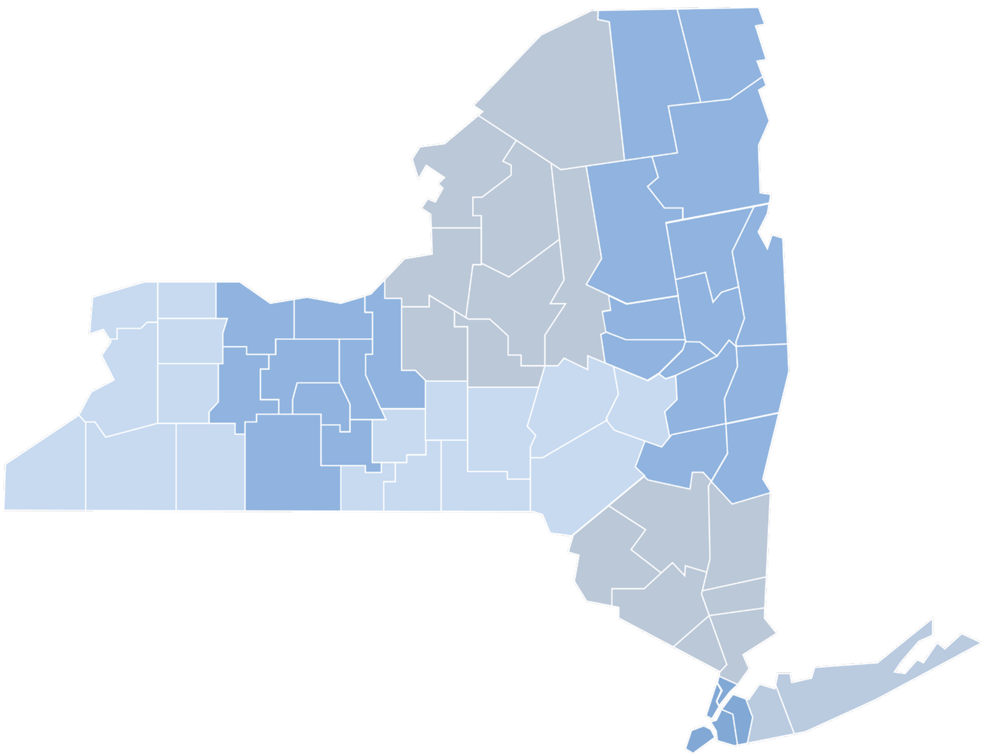
- We selected 15 of the 251 shared and generic accounts and inquired with OCM BOCES officials to determine the purpose of the accounts and whether the badges associated with the accounts were in the possession of responsible officials. If the badges were not in their possession, we inquired to determine why and attempted to locate the badges. We extended the review to all 251 accounts to identify their creation, and last used date and time as it appeared on the accounts list to determine whether all 251 accounts are currently in use and needed.

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

NYS FOLLOW US: osc.ny.gov/subscribe