New York State Comptroller
THOMAS P. DiNAPOLI

Orange-Ulster Board of Cooperative Educational Services

Building Access

July 2026 | Report S9-26-20
Prepared by the Division of Local Government and School Accountability

Table of Contents

Audit Results

Orange-Ulster Board of Cooperative Educational Services

Audit Objective

Did Orange-Ulster Board of Cooperative Educational Services (OU 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 March 11, 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 OU BOCES utilizes a building access management system (system) with 1,535 active building access accounts (accounts), including 1,414 devices issued to current employees, and 121 issued to non-employees, of which 21 are shared devices.[1] Each of the OU BOCES's eight 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

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

- 102 OU BOCES employees had two or more active badges, including six employees who were assigned as many as three active badges.
- 30 non-employee badges including four shared badges were not tracked or disabled when no longer needed.
- 28 active badges which OU BOCES officials could not locate, including 16 duplicate employee badges and three shared badges.

Although OU BOCES officials had a process for adding accounts in the system for employees and for non-employees, no one periodically reviewed active accounts to determine whether they were needed. Furthermore, although OU BOCES officials developed written procedures requiring the Safety and Security

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).

Department and the Technology Department to regularly review active badges to ensure individuals are promptly removed when access is no longer needed, the procedures were not effectively implemented and responsibilities for performing and documenting these reviews were not clearly defined.

This report includes four recommendations that, if implemented, will help OU BOCES officials improve management and monitoring of building access accounts and badges. OU BOCES 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 State Comptroller's (OSC's) authority as set forth in Article 3 of New York State General Municipal Law (GML). This audit's methodology and standards are included in Appendix C.

The OU BOCES Cooperative Board (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 OU BOCES' 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 we make available to local officials that can help them improve operations, are included in Appendix A.

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

During our fieldwork in March 2026, the OU BOCES had 1,535 active accounts associated with 1,414 badges issued to 1,306 current employees, and 121 badges issued to non-employees including 100 assigned to individuals and 21 shared badges. We determined:

- 8 percent of current employees had two or more active badges, and
- 25 percent of non-employee badges, were unneeded.
- 41 percent of the badges we requested to observe OU BOCES officials could not locate.

Employee Accounts – Of the 1,306 current employees, 102 employees (8 percent) were assigned two or more active badges, including six employees who were assigned three active badges.

The Director of Safety and Security and the Director of Technology told us that duplicate badges were issued when replacements were needed due to loss, malfunction or changes in job responsibilities. However, officials did not ensure that prior badges were deactivated when replacements were issued. As a result, multiple active badges remained associated with individual users.

We requested to observe 16 of the duplicate badges for 10 employees; however, officials could not locate any of the requested badges. After our audit inquiry, the Director of Technology deactivated all 16 duplicate badges.

Non-Employee Accounts – Of the 121 non-employee badges, we determined 30 active badges (25 percent), were unneeded. Of the 30 active unneeded non-employee badges:

- 26 badges were assigned to individual non-employees, such as security personnel, contracted service providers, Orange County Department of Aging employees and summer program staff.
- Four were shared badges for system implementation testing and to provide access for a contractor during construction.

We requested to observe a sample of 14 of the 30 unneeded badges, as well another 15 shared badges assigned to first responders. OU BOCES officials could not locate 12 of these badges (41 percent).

When we brought these issues to OU BOCES officials' attention, the Director of Safety and Security and the Director of Technology reviewed active accounts and deactivated all duplicate badges, accounts associated with lost badges, and the unneeded badge accounts, including the 30 non-employee badges we identified above. However, because these accounts remained active after access was no longer needed and officials could not locate the badges, there was an increased risk that individuals could gain unauthorized access to OU BOCES buildings. These issues occurred, in part, because OU BOCES officials did not have a process to ensure non-employee badges were returned or accounted for when access was no longer required.

Account Management and Monitoring Procedures – Although OU BOCES officials adopted written procedures for issuing and managing accounts and badges, including procedures requiring the Directors of Safety and Security Department and the Technology Department to regularly review badge access, these procedures were not effectively implemented. Additionally, other departments including Human Resources and Operations are involved in the access management process. However, responsibilities for managing and monitoring building access accounts were not clearly defined and the procedures did not include additional departments having responsibility for access management.

Specifically, OU BOCES officials did not define who is authorized to create accounts, who is responsible for monitoring active accounts and the process to revoke access, by deactivating unneeded accounts and collecting badges.

While OU BOCES officials have established processes for issuing badges to new employees and non-employees, including the use of badge request forms, key control activities over monitoring and removal of access were not in place or not operating effectively. For example, OU BOCES officials did not perform periodic reviews of active badge accounts to determine whether access remained appropriate. Officials told us they accessed the system on an as-needed basis (e.g., when incidents occurred), rather than conducting routine monitoring. As a result, account updates were not always made in a timely manner and there was a potential for unauthorized access to OU BOCES buildings.

Recommendations

OU BOCES officials should:

1. Ensure employees do not have duplicate badges.

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

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

OU BOCES is composed of 18 component school districts. OU BOCES provides instructional and support programs and services at eight locations within Orange and Ulster Counties.

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

The Operations Department's clerks utilize the system to print and issue badges to users which are then distributed either by them or department heads. The IT Director and an IT department staff member have administrative rights to activate, modify and deactivate accounts in the system. In addition, the Safety and Security Department is responsible for overseeing building security and reviewing badge access.

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.

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

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. 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.

Orange Ulster BOCES
4 Harriman Drive
Goshen, NY 10924
(845) 291-0100 Fax: (845) 291-0129
www.ouboces.org

July 21, 2026

Nicole A. Tomsen, Chief of Municipal Audits Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor Albany, NY 12236

Re: Orange-Ulster Board of Cooperative Educational Services - Building Access Draft Audit Report (Report S9-26-20)

Dear Ms. Tomsen:

On behalf of the Orange-Ulster Board of Cooperative Educational Services (OU BOCES), please accept this letter as our formal written response to the draft audit report regarding Building Access (Report 59-26-20}.

We would like to extend our appreciation to the Office of the State Comptroller and your audit team for their professionalism and time spent reviewing our building access controls procedures. While we believe our security protocols and layered physical security infrastructure have been robust, we appreciate the auditors bringing to our attention deficiencies in the way we manage and monitor building access accounts and devices.

We have carefully reviewed the draft report's finding that OU BOCES officials did not properly manage and monitor building access accounts and badges. We agree with the findings and accept the recommendations presented in the report. We acknowledge the importance of the recommended actions, which include:

1. Ensuring employees do not have duplicate badges.
2. Deactivating accounts and collecting associated badges as soon as they are no longer needed.
3. Developing written procedures that define who is responsible for managing and monitoring accounts, and periodically evaluating those procedures.
4. Developing a reconciliation process to review active accounts for the necessity and appropriateness of access.

As we review and develop updated procedures based on the aforementioned recommendations, we will submit a separate, formalized CAP detailing our implementation strategy for these recommendations within 90 days of the release of the final audit report, as required.

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

Thank you again for your constructive feedback, which provides us with an excellent opportunity to strengthen our internal controls and ensure a safe and secure environment for our students, teachers, staff, and visitors.

Mark P. Coleman
Assistant Superintendent

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 OU BOCES officials and reviewed Board policies to gain an understanding of the OU BOCES'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 OU BOCES's 1,535 active building access accounts list to the employee master list to determine whether all accounts were associated with current OU BOCES employees. We interviewed OU BOCES officials and reviewed relevant documentation to determine whether the building access accounts and badges assigned to non-employee users were necessary. For any unnecessary accounts, we inquired as to why they were not deactivated.

- We selected 19 out of 21 shared accounts and inquired with the respective OU BOCES officials responsible for these badges to determine whether the badges were in their possession. If the badges were not in their possession, we inquired to determine why and attempted to locate the badges. We used our professional judgment to exclude two shared accounts, because they had a one-year expiration date established by OU BOCES officials and were scheduled to expire when we received the building access account listing.

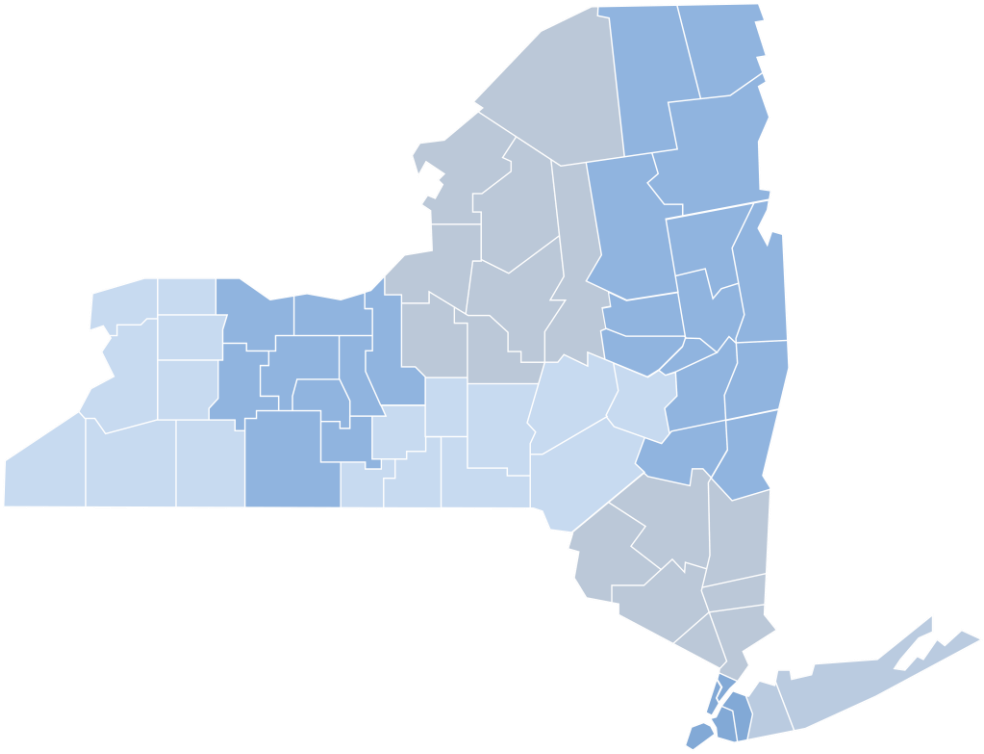
- We reviewed the active accounts list to determine whether any users had more than one account and badge and interviewed OU BOCES officials to determine why users would have duplicates. We identified 102 employees with a total of 108 duplicate badges. We used our professional judgment to select the 10 employees with the highest number of duplicate active badges, totaling 16 duplicate badges. We followed up with OU BOCES officials to observe all badges in their possession and determine why they had multiple access accounts and 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