New York State Comptroller
THOMAS P. DiNAPOLI

East Rochester Union Free School District

Building Access

August 2026 | S9-26-19
Prepared by the Division of Local Government and School Accountability

Table of Contents

Audit Results

East Rochester Union Free School District

Audit Objective

Did East Rochester 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 983 active building access accounts (accounts), including 337 devices issued to current employees and 646 issued to non-employees, of which 51 are shared devices.[1] The District's one school building has a single public point of entry. Employees may also access the building 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 the District school building, compromising building security and safety for students, teachers, staff and visitors. Specifically, of the accounts we reviewed, the District had active, but unneeded, accounts with assigned badges in the system:

- 88 individuals, including 62 employees and 26 non-employees had duplicate active badges, including 17 employees and four non-employees with three or more active badges.
- 126 badges (20 percent) of 646 non-employee accounts were unneeded.
- District officials could not locate 28 out of 52 (54 percent) requested badges.

Although District officials had an informal process for adding accounts in the system for employees and non-employees, no one periodically reviewed active accounts to determine whether they were needed. Furthermore, these issues occurred because District officials did not develop written policies and procedures for issuing and monitoring badges that clearly assign the roles and responsibility for managing and monitoring accounts.

This report includes four recommendations that, if implemented, will help District officials improve management and monitoring of building access accounts and badges. District officials generally agreed with our

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).

recommendations and their response is included in Appendix B. Appendix C includes our comments on issues raised in the District's 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 the New York State General Municipal Law (GML). The audit's methodology and standards are included in Appendix D.

The Board of Education (Board) has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report must be prepared and provided to OSC within 90 days, pursuant to Section 35 of GML, Section 2116-a (3)(c) of the New York State Education Law and Section 170.12 of the Regulations of the Commissioner of Education. To the extent practicable, implementation of the CAP must begin by the end of the next fiscal year. For more information on preparing and filing the CAP, please refer to the OSC brochure, *Responding to an OSC Audit Report*, which was provided with the draft audit report. The CAP should be posted on the District's website for public review.

Building Access: Finding and Recommendations

Properly managing and monitoring building access is a fundamental security function and the responsibility of school district officials. Various resources, publications and guides are available to help school district and Board of Cooperative Educational Services (BOCES) (together, "schools") officials develop and implement necessary building access infrastructure and systems to create a safe and secure environment for their students, teachers, staff and visitors.

More details on the criteria used in this report, as well as resources we make available to local officials that can help them improve operations, are included in Appendix A.

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

During our fieldwork in March 2026, the District had 983 active badges associated with 337 badges issued to 256 employees and 646 badges issued to non-employees, including 51 shared badges. We determined:

- 62 employees (24 percent) and 26 non-employees (4 percent) had two or more active badges, and
- 126 non-employee badges (20 percent) were unneeded.

Employee Accounts – Of the 256 current employees, 62 employees (24 percent) were assigned two or more active badges, including 17 employees who were each assigned three or more active badges.

We requested to observe badges of six employees that had three or more active badges, totaling 21 badges. District officials were unable to locate 10 of the 21 badges. The Director of Facilities (Director) explained that it was possible that active badges were mistakenly carried over from the District's former system when they upgraded in 2022 and these badges were not collected. When we brought these issues to District officials' attention, the Director deactivated all 10 unlocated badges.

Although the Director told us that while his assistant reviewed the personnel list every month and made employee access changes accordingly, no one verified whether this task was completed. In addition, District officials did not periodically compare active badge accounts to current employee records to ensure access was still needed. For example, the system has reports available that show periods of inactivity for badges which District officials could have reviewed to identify inactive or unnecessary badges.

Because District officials did not routinely review active accounts and badges, duplicate and unnecessary badges remained active, which increases the risk of unauthorized access to the District building.

Non-Employee Accounts – Of the 646 non-employee badges, we determined 126 active badges (20 percent) were unneeded. Of the 126 unneeded non-employee badges:

- 119 were assigned to individual non-employees, including 64 former employees, 19 former vendors, and eight community members to use the school facilities for non-school-related purposes (e.g., sports, band practice). The Director was unable to determine why the remaining 28 badges were issued.
- Seven shared badges including two for student teachers, two for contractors, one for coaches, one previously needed for system support, and one previously used for BOCES information technology (IT) support.

The Director told us District officials should have deactivated these accounts and collected the associated badges once they were no longer needed. However, the District did not have a formal process to ensure non-employee badges were returned or accounted for when access was no longer needed. Therefore, these

accounts and associated badges remained active, and as result, there was an increased risk of unauthorized access to District buildings.

In addition, 26 non-employees were issued two or more active badges, including four employees with three or more active badges. We requested to observe the badges of four non-employees that had three or more active badges, totaling 13 badges. District officials were unable to locate four of these badges. The Director told us that District officials should have considered these four badges lost, and immediately deactivated them. When we brought these issues with badges to District officials' attention, the Director reviewed active accounts and deactivated all unneeded duplicate, former employee, vendor and shared badges.

These issues occurred, in part, due to a lack of clear responsibilities and documented procedures for managing and monitoring building access, including regularly reviewing system-generated access reports, reconciling active accounts to current authorized users and promptly deactivating accounts when access was no longer needed.

Account Management and Monitoring Procedures – Although District officials had informal procedures in place for issuing and managing badges, they did not establish written procedures for issuing, managing and monitoring accounts. Specifically, District officials did not define who is authorized to create accounts, who is responsible for monitoring active accounts and the process to change/revoke access, including deactivating unneeded accounts and collecting those badges.

At the time of our fieldwork, there were four District employees involved in access management, with each having access to the system allowing them to create, change and revoke badge access, including the Director, IT Director and two additional employees. The Director told us requests to create, change or revoke access were generally communicated informally, either in person or by email. However, there was no formal approval process or written documentation maintained for verbal requests.

The Director also told us that employee access changes were generally based on monthly personnel reports presented at Board meetings and communication from Human Resources or the Superintendent. However, no one verified that access updates were completed, and there was no periodic reconciliation of active accounts and badges to employee or non-employee records to determine whether access remained appropriate. As a result, necessary access updates were not made in a timely manner and there was a potential for unauthorized access to the District building. In addition, badges were not always collected, as there was no process in place to ensure unneeded badges were returned or destroyed.

Recommendations

District officials should:

1. Ensure employees do not have unneeded 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

The District's boundaries include the Town of East Rochester and parts of the Towns of Perinton and Pittsford in Monroe County. The District's school building is in the Town of East Rochester.

The District is governed by the elected five-member Board. The Board is responsible for managing and controlling the District's financial and educational affairs. The Superintendent is responsible, along with other administrative staff, for managing the District's day-to-day operations under the Board's direction.

The Superintendent assigned the Director the responsibility for managing and monitoring accounts. The Director, IT Director and two assistants had full access to the system to print badges and activate, modify and deactivate user access accounts. Badges were distributed to individuals directly or department heads. The Director and the IT Director had administrative rights to the system.

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 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.

East Rochester School District
222 Woodbine Ave.
East Rochester, NY 14445
(585) 248-6302 Fax: (585) 586-3254
Website: http://www.erschools.org

July 30th, 2026

To: New York State Office of the State Comptroller
From: Scott Wilcox, Superintendent of Schools
RE: Building Access Audit – Response and Corrective Action Plan
Cc: Board of Education, Audit Committee

Following a comprehensive review of audit report S9-26-19 from the Office of the State Comptroller, the East Rochester Union Free School District offers the following Response and Corrective Action Plan:

Response:

The District extends its gratitude to the Office of the State Comptroller for their statewide efforts to provide needed audit and oversight services to a functional area of school operations which has seen significant changes in recent years. The use of new and emerging technologies, the need to balance community engagement with risk tolerance, and the presence of shifting demographics - such as increased workforce mobility and evolving population stability - have culminated in a need to revisit school building access practices to ensure the continued safety of the students, communities and staff who frequent public school buildings day in and day out.

East Rochester Schools welcome the recommended improvements as opportunities to further layer upon our existing, comprehensive security and safety practices which include:

- A dedicated and fully-staffed, secure, single point of entry [OSC Comment: See Appendix C, Note 1]. Constructed in 2020, this entry allows the district to fully vet all visitors, and to create a physical separation between students and visitors until such time that the visitors have received full clearance to enter the building.

- The replacement of a legacy electronic access system with a modern system that allows for the type of oversight and reporting that supports both the OSC's audit as well as future, regularly scheduled internal audits.

- A 2024 district-wide rekeying project which dramatically enhanced access control within our building, matching access privileges with organizational need.

- A Campus-Wide Emergency Notification System which allows the district to immediately provide information and directions to all building occupants in an emergency.

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

- Routine camera surveillance upgrades, consistent evaluation and improvements to door monitoring and access systems, routine hallway patrols, consistent School Resource Officers' presence, and collaborative arrangements with both the East Rochester Police Department and the Monroe County Sheriff's Office to grant building access to duly sworn law enforcement officers.

As it relates to the single Audit finding, Finding 1, that "District officials did not properly manage and monitor building access accounts and badges," the District generally agrees that there are significant opportunities for improvement. While such actions already taken and planned will be shared as part of the corrective action plan, the District finds that important context regarding the 126 unneeded badges helps to more appropriately illustrate the district's true risk profile. Specifically, of these 126 badges:

- 23 (18%) belonged to duly sworn law enforcement officers.
- 50 (40%) were not badges, but access fobs. These fobs were active in the system due to an erroneous data import that occurred during a migration from an old system. Historical administrative practices strongly support the conclusion that these obsolete access devices were previously disposed of [OSC Comment: See Appendix C, Note 2].
- 2 were functionally inactive due to all access privileges being previously revoked.
- The district promptly deactivated all unneeded badges upon discovery of their active status. This is also true of all badges that the district was not able to promptly produce at the OSC's request, including those of employees and sworn law enforcement officers.
- There have been zero documented instances of unneeded credentials being used to gain entry identified through the various other security practices the district has in place. Such practices include the use of a secure single point of entry, video surveillance, and security personnel monitoring.

Noting opportunities for improvement discovered through the audit and as shared with the district at the June 17th Summary of Findings meeting, the District offers the following Corrective Action Plan:

Corrective Action Plan:

Recommendation #1: Ensure Employees do not have unneeded duplicate badges.

As of May 15th, 2026, the District has established a written framework for the issuance of badges. This framework outlines the access privileges to be provided to various users based on organizational need. Duplicate badges require written justification outlining a legitimate business case for their need. The approval process uses an electronic form submission which requires multiple layers of administrative approval prior to the issuance of badges. The District is actively using this new process.

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

As of August 1st, 2026, the Human Resources Office will complete an electronic form submission upon separation of employment, which initiates the deactivation of employee accounts. The district will require employees to return badges, providing clear instructions along with final separation notices. Badges held by those other than regular, full-time employees are programmed to expire in accordance with the written framework and based upon the period of needed access. The destruction of unneeded badges is noted in the individual user records within the access software system.

Recommendation #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.

As of May 15th, 2026, written procedures have been established for the management of badge access accounts. The procedures include defined roles and separation of duties to ensure that no single individual has autonomy in the process. Roles include Requestors, Approvers, Access Administrator, Printer, and Issuer. The written procedures establish a digital audit trail and approval process, specific access privileges to be granted based upon organizational need, pre-programmed expiration dates for temporary access needs, and a routine process to periodically evaluate and adjust based on need.

Recommendation #4: Develop a reconciliation process utilizing system reports, and review active accounts for necessity and appropriateness of access.

As of May 15th, 2026, a routine credential and database verification plan has been established, requiring the Director to complete a bi-annual credential and database verification, cross-checking the Active Credential Audit from the **[Redacted]** management system against law enforcement lists, employee rosters, and community users. The next internal audit is scheduled for October 2026. This process, in combination with the processes and procedures established in response to recommendations 1-3, ensure comprehensive oversight and management of the electronic access system.

The District expresses its appreciation to the Office of the State Comptroller for its review and recommendations regarding best practices in building access. We remain committed to maintaining the highest levels of safety and security across our campus and will continue to pursue continuous improvement in all facets of student and staff safety.

Appendix C: OSC Comment on the District's Response

Note 1

The District's one school building has a single public point of entry. However, employees may also access the building through additional entry points, using a device for entry. As stated in our report, during our fieldwork 62 District employees had duplicate active badges, including 10 badges which District officials could not locate when requested.

Note 2

Devices such as "access fobs" can allow for the same building access as a badge and, therefore, unneeded devices increase the risk of unauthorized access. Furthermore, District officials were unable to provide supporting documentation that the devices were collected or destroyed. These devices were still active in the District's system at the start of the audit.

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 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 983 active accounts list to the employee master list to determine whether all accounts were associated with current District employees. We also compared the accounts list to reports of current police officers and sheriff's deputies provided by local law enforcement. We interviewed District officials and reviewed relevant documentation to determine whether the accounts and badges assigned to non-employee users were necessary. For any unnecessary accounts, we inquired as to why they were not deactivated.

- We used our professional judgment to select 12 out of 119 unneeded non-employee badges based on user category and last access date. We 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 used a random number generator to select six out of 51 shared accounts 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.

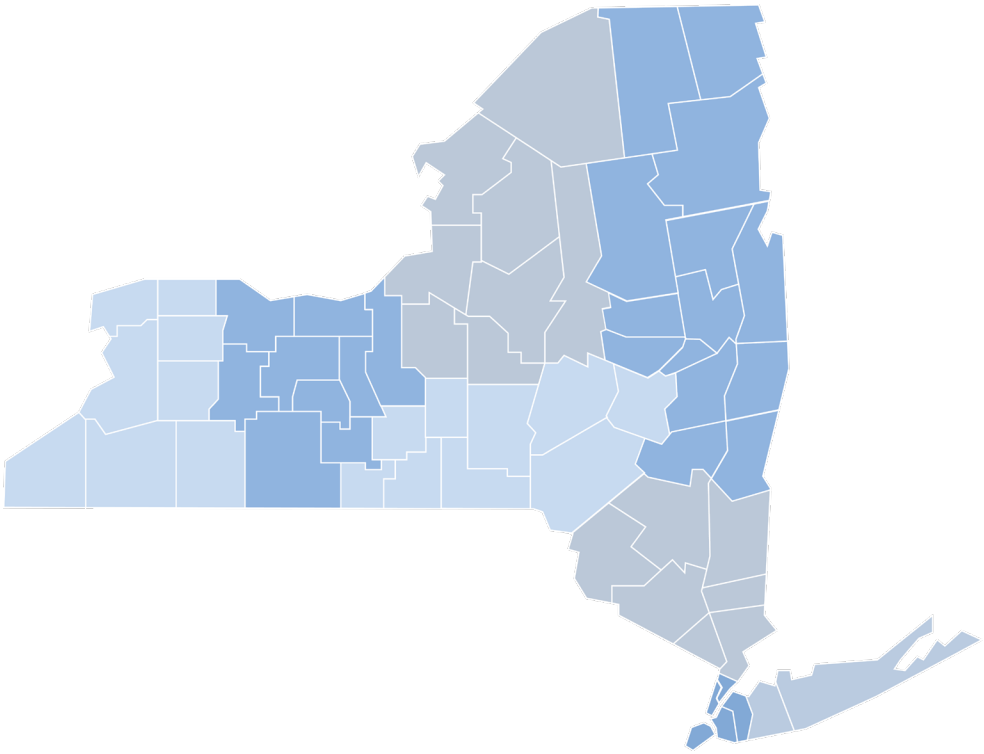
- We reviewed the active building accounts list to determine whether any users had more than one account and badge and interviewed District officials to determine why users were assigned more than one account. We identified 88 individuals (62 employees, 26 non-employees) with a total of 113 duplicate badges (82 employees, 31 non-employees). We discussed these duplicate badges with District officials to determine why individuals had multiple badges. We used our professional judgment and selected six employees with three or more duplicate badges, totaling 21 badges, and four non-employees with three or more duplicate badges, totaling 13 badges, and followed up with District officials to observe all badges sampled.

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

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

Questions?

STATEWIDE AUDITS
Nicole A. Tomsen, Chief of Municipal Audits
295 Main Street, Suite 1032 • Buffalo, New York 14203-2510
Tel (716) 847-3647 • Fax (716) 847-3643
Email: Muni-Statewide@osc.ny.gov



Contact

Office of the New York State Comptroller
110 State Street
Albany, New York 12236

(518) 474-4044

www.osc.ny.gov

Prepared by the Division of Local Government and School Accountability