FILE NO. 917-2025

OHIO AUDITOR OF STATE
KEITH FABER

65 East State Street
Columbus, Ohio 43215
ContactUs@ohioauditor.gov
800-282-0370

MANAGEMENT LETTER

RECEIVED by the Office of the City Clerk, Clerk of Council, City of Cleveland on July 14, 2025

City of Cleveland
Cuyahoga County
601 Lakeside Avenue
Cleveland, Ohio 44114

To the Honorable Mayor Justin M. Bibb, Members of City Council, and the Audit Committee:

We have audited, in accordance with auditing standards generally accepted in the United States and the Comptroller General of the United States' *Government Auditing Standards*, the financial statements defined in our Independent Auditor's Report of the City of Cleveland, Cuyahoga County, Ohio (the City) as of and for the year ended December 31, 2024, and the related notes to the financial statements and have issued our report thereon dated June 26, 2025.

Government Auditing Standards require us to communicate deficiencies in internal control, as well as report on compliance with certain provisions of laws, regulations, contracts and grant agreements that could directly and materially affect the determination of financial statement amounts. We have issued the required report dated June 26, 2025, for the year ended December 31, 2024.

2 CFR Part 200 subpart F requires that we report all material (and certain immaterial) instances of noncompliance, significant deficiencies, and material weaknesses in internal control related to major federal financial assistance programs. We have issued the required report dated June 26, 2025, for the year ended December 31, 2024.

We are also submitting the following comments for your consideration regarding the City's compliance with applicable laws, regulations, grant agreements, contract provisions, and internal control. The comments reflect matters that do not require inclusion in the *Government Auditing Standards* or Single Audit reports. Nevertheless, the comments represent matters for which we believe improvements in compliance or internal controls or operational efficiencies might be achieved. Due to the limited nature of our audit, we have not fully assessed the cost-benefit relationship of implementing the recommendations. The comments reflect our continuing desire to assist your City but are only a result of audit procedures performed based on risk assessment procedures and not all deficiencies or weaknesses in controls may have been identified. If you have questions or concerns regarding the comments please contact your regional Auditor of State office.

Recommendations

1. Inventory Reporting

In our audit engagement letter, as required by AU-C Section 210, Terms of Engagement, paragraph .06, management acknowledged its responsibility for the preparation and fair presentation of their financial statements; this responsibility includes designing, implementing and maintaining internal control relevant to preparing and fairly presenting financial statements free from material misstatement, whether due to fraud or error as discussed in AU-C Section 210 paragraphs .A14 & .A16. Governmental Accounting Standards Board (GASB) Cod. 1100 paragraph .101 states a governmental accounting system must make it possible both: (a) to present fairly and with full disclosure the funds and activities of the governmental unit in conformity with generally accepted accounting principles, and (b) to determine and demonstrate compliance with finance-related legal and contractual provisions.

Due to insufficient knowledge regarding the operation of the Division of Water Pollution Control inventory reporting system, the Department of Utilities Division of Water Pollution Control utilized a report dated in April 2025 to report its inventory as of December 31, 2024. This resulted in an overstatement of Materials and Supplies totaling $292,000. The City subsequently adjusted the Division of Water Pollution Control's financial statements for this error.

Lack of sufficient training over complex systems can lead to inaccurate reporting and potential mispostings on the financial statements.

The City should establish procedures to ensure that the necessary reports are run at the appropriate time in order to ensure that financial statements reflect accurate balances.

2. IT – Security Administration

Security administration helps to ensure computer resources are only provided to users on an as needed basis and according to management's intentions. Effective security administration policies and procedures typically include on-boarding procedures to confirm initial user access is appropriate, periodic review of user access for appropriateness.

Payroll Application:

- While new user access to the payroll application requires a signed authorization form which details module access within the application, the actual assignment of the access within the application is not based on a predefined role or group, rather each individual task within a module needs to be manually keyed in for the new user. The City noted the application does easily allow for the creation of predefined roles due to fact the same role/access would need to be created for each division/department.
- Nine HR employees require elevated access during general wage increase sessions to perform job duties. Due to payroll application setting restrictions, these users are given full access to the system during the general wage increase sessions, which is beyond their normal job duties.
- Due to payroll application software security restrictions, limited staff from both payroll and HR have full access to the application. This access would allow employees from both divisions to create new users and edit payroll data.

Active directory:

- 17 service accounts had admin access that was no longer required.

Recommendations
(Continued)

2. IT – Security Administration (Continued)

When security authorization documentation does not provide detailed information regarding the roles and privileges provided within the application, there is an increased risk of unauthorized access to data. The practice of "mirroring" access for users within an application can be especially risky if the account being "mirrored" was previously granted higher level privileges than would be necessary for the new user. In addition, accounts with excessive access may result in the accidental or intentional loss of or damage to data.

The City should develop and implement the following security administration controls:

- Require on-boarding support to identify the specific responsibility and security group access a user should be assigned within an application rather than stating access be based on an existing employee's ability.
- Enforce the principal of least privileged access over all critical systems to ensure staff only have access to specific data and resources needed to perform their job responsibilities.
- Periodically review service account privileges to ensure they are still reflecting active needs

3. IT – Cybersecurity Training

Sound controls require regular security awareness training. Establishing a security awareness training program is an effective way to ensure employees are aware of cyber threats so they will not make costly errors that could result in a security incident or data breach. Encouraging awareness about data protection and security issues while developing properly trained staff requires that various areas be addressed through a comprehensive training program.

Security awareness training initiatives can include classroom or webinar style sessions, security awareness web sites, helpful hints provided via email, and bulletin board notices. These methods can help ensure employees have a solid understanding of security policies, procedures, and best practices and what they can do to recognize and respond appropriately to potential security issues and cyber threats.

The City has a formal cyber security policy; however, the enforcement of the policy was not consistent across all City departments.

Without adequate training, users may not understand security risks and their role in mitigating those risks.

The City should establish a cybersecurity awareness training program for all network users. Participation in such training should be required, tracked and enforced to help ensure all employees receive training on a regular basis.

Recommendations
(Continued)

4. IT – Logical Access (City Hall, DPU and Municipal Court)

Logical access controls are critical to help ensure computer resources are appropriately protected. Passwords are typically used to authenticate a user before access is granted to the computer system. Multifactor (MFA) authentication, in which a user is required to provide two or more verification factors to gain access to critical data, and strong password policies are key controls in preventing unauthorized user access. In addition, monitoring user access activity via security reports help to identify suspicious activity.

While the City Hall, Department of Public Utilities (DPU) and Municipal Court IT environments have strong password controls in place to restrict user access to critical systems, MFA authentication policies were not in place over the DPU and Municipal Court IT environments and the MFA policies did not apply to general users accessing the network internally for City Hall users.

In addition, the following logical access issues were noted over the City's time keeping application:

- The password policy for one high level group is set to never expire.
- The vendor hosted application has a complementary user entity control that encourages user entities to monitor the system's security report and communicate suspicious activity. The City is currently not reviewing security reports over on a regular basis.

When strong password and MFA policies are not implemented or enforced, there is an increased risk of unauthorized access to data. In addition, the risk of inappropriate access or unauthorized changes increases when audit reports are not reviewed on a regular basis.

The City, DPU and the Municipal Court should enforce strong password policies and consider implementing multifactor authentication policies over all significant systems and applications.

Additionally, the City should review the SOC 1 Type 2 reports for their service organizations and ensure they are meeting the Complementary User Entity Controls listed in each.

We intend this report for the information and use of the City Council, audit committee, and management.

Keith Faber
Auditor of State
Columbus, Ohio

June 26, 2025