CLARK SCHAEFER HACKETT
BUSINESS ADVISORS

One East Fourth Street, Suite 1200, Cincinnati, Ohio 45202
P. 513.241.3111 | F. 513.241.1212

To the Honorable Mayor and Members of the City Council
City of Cincinnati, Ohio:

In accordance with *Government Auditing Standards* applicable to financial audits, we have audited the financial statements of the City of Cincinnati (the "City"), as of and for the year ended June 30, 2024, and have issued our report thereon dated December 30, 2024.

Government Auditing Standards also require that we describe the scope of our testing of compliance with laws and regulations and internal control over financial reporting and report any irregularities, illegal acts, other material noncompliance and significant internal control deficiencies. We have issued the required report dated December 30, 2024, for the year ended June 30, 2024.

Uniform Guidance requires that we report all material (and certain immaterial) instances of noncompliance and significant deficiencies in internal control related to major federal financial assistance programs. We have issued the required report dated December 30, 2024, for the year ended June 30, 2024.

We are also submitting for your consideration the following comments on the City's compliance with applicable laws and regulations and on its internal controls. These comments reflect matters that, while in our opinion do not represent material instances of noncompliance or significant internal control deficiencies, we believe represent matters for which 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 suggested below. However, these comments reflect our continuing desire to assist the City. If you have any questions or concerns regarding these comments, please do not hesitate to contact us.

Fraud Reporting New Hires

The Auditor of State of Ohio (AOS) has created training material detailing Ohio's fraud reporting system and the means of reporting fraud, waste, and abuse. Pursuant to Ohio Rev. Code § 117.11, each new employee or elected official is required to confirm receipt of this material within thirty days after taking office or beginning employment. The AOS has provided a form to be printed and used by public employees and elected officials to sign and verify their receipt of information material as required by this statute. During our testing of new employees, it was determined that the City could not provide the required documentation for four of the ten employees selected for testing. We recommend the City review its current policies and procedures related to new employee onboarding to ensure compliance with Ohio Rev. Code § 117.11.

Management's Response: The City of Cincinnati has implemented significant measures to address the issues noted in last year's Audit Management Letter. All new hires are now required to complete the Ohio Ethics Commission Online Training, review fraud reporting documents, and sign the Fraud Reporting Acknowledgment Form within 30 days of hire. Additionally, a citywide compliance initiative was launched this summer to ensure all employees and elected officials completed the updated training required by Ohio Revised Code § 117.103 by the September 28, 2024, deadline.

Information Technology

Disaster Recovery Plan

Per inquiry with City of Cincinnati ETS CISO, we noted that there is no formal City-wide Business Continuity/Disaster Recovery plan in place for all departments to follow. Lack of a City-wide Disaster Recovery Plan and/or Business Continuity Plan can expose the organization to data loss, prolonged downtime, financial setbacks, and reputational damage.

The City should consider implementing a city-wide disaster recovery plan and/or business continuity plan that involves collaboration among government agencies, businesses, and community stakeholders. It should encompass risk assessments, clear communication channels, resource allocation, regular drills, and technological redundancies to ensure swift responses, minimize disruptions, and safeguard the well-being of citizens and critical infrastructure during emergencies.

Management's Response: ETS recognizes the importance of a comprehensive city-wide disaster recovery and business continuity plan. Through IT governance, we will conduct a thorough assessment of current practices, identifying key vulnerabilities, communication gaps, and resource constraints. Based on these findings, we will develop a phased plan to strengthen disaster response capabilities, focusing initially on the most critical vulnerabilities and integrating measures like risk assessments and technological redundancies.

This initiative is linked to the ongoing IT asset management project, which is expected to conclude in January 2025. Our ability to progress will depend on the availability of resources for technological redundancies. A detailed roadmap will be developed, and the assessment will begin within this fiscal year. Enforcement and monitoring will occur through governance and policies.

Access Control

We noted that user access reviews for standard users, administrators, and VPN/Remote access are not formally documented or performed on a periodic basis. Not performing periodic user access reviews poses significant security risks. Without these reviews, there's a higher chance of unauthorized access, insider threats, and compromised system integrity. It can lead to data breaches, misuse of privileges, and vulnerabilities in critical systems, potentially resulting in severe financial losses and reputational damage for the organization.

The City should consider establishing a structured process for regular assessments of user permissions, segregating duties, and documenting access privileges. This includes leveraging automated tools for continuous monitoring, defining clear roles and responsibilities, and enforcing a regular review cadence to ensure adherence to security policies while minimizing risks associated with unauthorized access and maintaining data integrity.

Management's Response: ETS acknowledges the need for a structured approach to assess user permissions and segregate duties. We will conduct a comprehensive review of current access control protocols, focusing on user permissions, roles, data segregation, and documentation. Based on this assessment, we will develop a phased plan to strengthen our access control framework, addressing immediate vulnerabilities and creating a roadmap for long-term improvements.

This initiative is tied to the ongoing IT asset management project, set for completion in January 2025. Progress will depend on available resources for technology solutions and staffing. A supporting policy will be developed within this fiscal year.

Encryption

We noted that there is a lack of a formal city-wide encryption policy enforcing all devices to be configured with storage encryption. In addition, per inquiry with ETS CISO, it was noted that not all stored data is encrypted at-rest for CFS, CMI, and CHRIS. Lastly, backup data over the internal local network is not currently encrypted in-transit; however, over the external network the backup data is encrypted. Not having a formal encryption policy that mandates storage encryption on devices poses a significant risk of data exposure in case of loss or theft. Additionally, without encryption on all data at-rest and in-transit, sensitive information stored on these devices becomes easily accessible, potentially leading to data breaches, compliance violations, legal repercussions, and damage to the organization's reputation.

The City should consider implementing a formal encryption policy for storage across devices to safeguard sensitive data from unauthorized access in case of loss or theft, mitigating the risks of data breaches, compliance violations, and reputational damage. In addition, the City should review the encryption protocols for sensitive data at-rest and in-transit and regularly update encryption protocols, conduct

vulnerability assessments, and enforce strict access controls to maintain data security comprehensively across storage and transmission.

Management's Response: ETS acknowledges the critical importance of securing sensitive data through encryption and will develop a formal encryption policy. The policy will define a data classification framework, establish encryption standards for each level, and provide implementation guidelines for devices and storage systems, with a focus on a tailored approach based on data classification.

This initiative is contingent upon having the necessary technology to enforce the policy. The required technology will be implemented as part of the funded ETS Centennial II data center refresh project, scheduled to begin in January 2025. A formal encryption policy will be developed within this fiscal year.

We will review the status of these comments during our next audit engagement. We have already discussed these comments and our suggestions with Management, and we will be pleased to discuss them in further detail at your convenience, to perform any additional study of these matters, or to assist you in implementing the recommendations.

This report is intended solely for the information and use of the Mayor, Members of City Council, the City's management, others within the City, and the Auditor of the State of Ohio and is not intended to be and should not be used by anyone other than these specified parties.

Clark, Schaefer, Hackett & Co.

Cincinnati, Ohio
December 30, 2024