

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, 2023, and have issued our report thereon dated December 29, 2023.

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 29, 2023, for the year ended June 30, 2023.

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 29, 2023, for the year ended June 30, 2023.

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.

Subrecipient Monitoring

In accordance with Uniform Guidance (UG) §200.332 (Requirements for pass-through entities), the City is required to monitor the activities of its subrecipients to ensure their accountability and compliance with federal statutes, regulations, terms and conditions of the subaward, and that subaward performance goals are achieved. During our testing of both the Coronavirus State and Local Fiscal Recovery Funds (CSLFRF) and Emergency Rental Assistance programs, it was determined the City only requires its subrecipients to provide the annual audit documentation during the close out period of the applicable grant.

We recommend the City review and update its current policy to require subrecipients to submit audit documentation annually to ensure timely remediation of any potential deficiencies noted.

Management's Response: The City will implement additional oversight and procedures to ensure that all subrecipient's are submitting their Single Audits or when applicable documentation as to why they were not required to have a single audit when reporting to the City each audit cycle

CSLFRF Quarterly Reporting

During testing of the quarterly reports for the CSLFRF program filed with the U.S. Department of the Treasury, we noted certain inconsistencies related to how the City reported contractors and subrecipients within the "Subaward Type" line item. Although the City correctly updated a majority of these items in the subsequent quarter report, we recommend the City implement additional oversight and review procedures over CSLFRF reporting prior to submission to ensure pass through recipients are appropriately identified and reported within program guidelines.

Management's Response: The City will implement additional oversight when reporting to the U.S. Department of Treasury and seek additional guidance and/or clarification when questions arise before submission of reports to ensure all recipients are accurately identified and reported within the Treasury portal.

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 two 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's Human Resources Department (HR) is in the process of reviewing our onboarding process to ensure that all newly hired employees and elected officials receive the required form provided by the AOS and is signed acknowledging receipt. Additionally, the City will provide refresher training to all individuals that are responsible for new employee onboarding to ensure they are providing the required materials and obtaining newly hired employees signatures on the AOS form.

City Charter Compliance

All elected officials and city employees whose positions involve a substantial and material exercise of administrative direction in the formulation of public policy, expenditure of public funds, enforcement of laws and rules shall file an annual financial disclosure statement with the Clerk of Council by April 15th for the preceding calendar year. The required elements of the disclosure are stipulated in Sec. 3 of Article XXVI. During testing of this requirement, it was determined that none of the ten individuals selected for testing filed annual financial disclosure statements by the statutory deadline of April 15, 2023. We recommend the City implement procedures to ensure all disclosures are received by the required deadline.

Management's Response: The City of Cincinnati's Human Resources Department (HR) will implement procedures to ensure compliance with the statutory deadline for annual financial disclosure statements with the Clerk of Council by April 15th each year.

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 acknowledges the necessity of a city-wide disaster recovery/business continuity plan. Through IT governance, we will conduct a thorough assessment of current practices, identifying vulnerabilities, communication gaps, and resource limitations. Based on this, we will create a phased plan to enhance disaster response capabilities, prioritizing critical vulnerabilities and incorporating suggested measures like risk assessments and technological redundancies.

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 recognizes the need for a structured process to assess user permissions and segregate duties. We will comprehensively review current access control protocols, analyzing user permissions, roles, data segregation, and documentation. Through this assessment, we will develop a phased plan to strengthen our access control framework, prioritizing immediate vulnerabilities and outlining a roadmap for long-term improvements.

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 agrees on the importance of securing sensitive data through encryption and will develop a formal encryption policy. This policy will define a data classification framework, encryption standards for each level, and implementation guidelines for devices and storage systems, recognizing the need for a nuanced approach based on data classification.

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 29, 2023