Dave Yost • Auditor of State

MANAGEMENT LETTER

City of Cincinnati
Hamilton County
801 Plum Street
Cincinnati, Ohio 45202

To the Honorable Mayor and Members of the City Council:

We have audited the financial statements of the City of Cincinnati, Hamilton County, Ohio (the City) in accordance with *Government Auditing Standards*, as of and for the year ended June 30, 2014, and have issued our report thereon dated February 26, 2015, wherein we noted the City has implemented the provisions of GASB Statement 67.

Government Auditing Standards require us to report significant internal control deficiencies, fraud, (including noncompliance with laws and regulations), and also abuse and noncompliance with contracts and grant agreements that could directly and materially affect the determination of financial statement amounts. We have issued the required report dated February 26, 2015, for the year ended June 30, 2014.

Office of Management and Budget Circular A-133 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 February 26, 2015, for the year ended June 30, 2014.

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. These comments reflect matters that do not require inclusion in the *Government Auditing Standards* or Office of Management and Budget Circular A-133 reports. Nevertheless, these 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 these recommendations. However, these comments reflect our continuing desire to assist your City. If you have questions or concerns regarding these comments please contact your regional Auditor of State office.

COMPLIANCE

1. **Ohio Rev. Code, § 149.351,** states that all records are the property of the public office and shall not be removed, destroyed, mutilated, transferred, or otherwise damaged or disposed of, in whole or in part, except as provided by law under the rules adopted by the records commission provided for under sections 149.38 to 149.42 of the Revised Code.

   The following records were not provided for audit:

   - 6 out of 45 (13%) federal tax withholding forms (W-4),
   - 9 out of 45 (20%) state tax withholding forms,

COMPLIANCE
(Continued)

- 1 out of 41 (2.4%) city retirement form,
- Construction in progress supporting documentation related to the TIFF Funds project

Failure to maintain the required forms could result in an employee disputing deductions from payroll earnings. Failure to maintain adequate documentation for construction in progress could result in inaccurate financial statements. The City should maintain all records as required by **Ohio Rev. Code § 149.351.**

2. *__Ohio Rev. Code, §117.103 (B) (1),__ states a public office shall provide information about the Ohio fraud-reporting system and the means of reporting fraud to each new employee upon employment with the public office. Each new employee shall confirm receipt of this information within thirty days after beginning employment. The auditor of state shall provide a model form on the auditor of state's web site (https://ohioauditor.gov/fraud/FraudReportingSystemModelForm.pdf) to be printed and used by new public employees to sign and verify their receipt of information as required by this section. The auditor of state shall confirm, when conducting an audit under section 117.11 of the Revised Code, that new employees have been provided information as required by this division.

Seven out of Fourteen (50%) new hires did not complete the fraud reporting forms acknowledging they are aware of the fraud reporting system.

Failure to notify employees about the fraud-reporting system and have them acknowledge the confirmation of notification could lead to fraud not being reported. The City should adopt procedures to make sure that all new hires complete and submit the appropriate fraud reporting forms.

3. **OMB Circular A-133, Subpart C, Section .300(a)** states that the auditee shall identify, in its accounts, all Federal awards received and expended and the Federal programs under which they were received. Federal program and award identification shall include, as applicable, the CFDA title and number, award number and year, name of the Federal agency, and name of the pass-through entity.

The determination of when a federal award is expended should be based on when the activity related to the award occurs. Generally, the activity pertains to events that require the non-Federal entity to comply with laws, regulations, and the provisions of contracts or grant agreements, such as: expenditure/expense transactions associated with the grants.

The City maintained records accounting for the amounts reported on the Schedule of Federal Expenditures. However for four of the funds listed below we were unable to agree some of the amounts listed on the Schedule of Federal Expenditures back to the City's General Ledger or Trial Balance. We were able to agree these amounts to other supporting documentation.

Fund	Fund Name	SEFA Category Reported
304	Community Development Block Grant	Contributions and Other Revenue
980	Capital Projects	Grant and Contract Revenue Received
350	Public Health Research	CFS Expenditures
980	Capital Projects	CFS Expenditures

COMPLIANCE
(Continued)

Failure to separately account for federal funds in the City's general ledger reduces the accountability over federal expenditures and reduces the ability to monitor compliance with federal grant requirements. The City should separately account for federal funds in the City's general ledger.

4. **2 CFR section 180.300** states that when a non-federal entity enters into a covered transaction with an entity at a lower tier, the non-federal entity must verify that the entity is not suspended or debarred or otherwise excluded. This verification may be accomplished by checking the Excluded Parties List System (EPLS) maintained by the General Services Administration (GSA), collecting a certification from the entity, or adding a clause or condition to the covered transaction with that entity.

   The City entered into contracts with three out of seven (43%) vendors that were not checked against the EPLS database to ascertain the covered transactions or sub awards were not awarded to suspended or debarred parties nor were signed statements from the vendor obtained.

   The City did not have evidence that the EPLS was checked, that a certification from the entity was obtained, or that adding a clause or condition to the covered transaction was completed. The City should review the EPLS and maintain documentation of the review.

5. **General Section, Section VI, Award Administration Information C7 of the HUD Administrative Agreement** states the applicant must collect demographic data by using the HUD approved Race/Ethnic Form (HUD-27061), in accordance with the requirements of the General Section, Section VI, Award Administration Information C7.

   Sixteen of the forty (40%) cases tested represented an occupied unit for which HUD form HUD-27061-H, race and ethnic data was required but not present in the files. The City should maintain documentation of all required demographic data.

RECOMMENDATIONS

1. ***Disaster recovery (City of Cincinnati, and Cincinnati Retirement System)**

   In order to ensure minimal disruption to the services it provides, the City and the Retirement System should maintain a disaster recovery plan that identifies procedures to perform which facilitate the City's continued processing of information in the event of a disaster.

   The City did not have a formal disaster recovery plan documenting processes/procedures to follow in the event of a disaster.

   Without an adequately documented disaster recovery plan with contingency arrangements for alternate processing, the City may experience considerable and untimely delay in restoring its data processing functions following a disaster.

   The City should develop a formal disaster recovery plan. Upon its completion the plan should be tested and updated periodically to ensure its applicability to the City's data processing function.

RECOMMENDATIONS
(Continued)

The plan should include, but is not limited to the following:

- assessment of mission critical systems/prioritization of software applications
- team member contact information
- team member responsibilities
- vendor contact information
- evaluation of damages/planned contingency measures
- hot site designation
- hardware profile needs
- data backup and restore procedures

2. ***Password Configuration**

Active Directory is used for enterprise-wide authentication and access controls for Pension Gold. The current configuration requirements for passwords and account lockout are inconsistent with industry "best practice" standards. Pension Gold is hosted and maintained by the application vendor, which uses Active Directory for authentication and access controls.

The vendor requirements for passwords are inconsistent with industry "best practice" standards. Deviations from industry best proactive standards may reduce the overall security and integrity of the data within in the systems.

We recommend that the City assess the risk associated with the current password requirements and account lockout settings. Additionally, in order to effectively protect Pension Gold data, City management should work with the application vendor to determine whether the password configuration can be strengthened.

3. Levi, Ray and Shoup Applications – Lack of SOC 1 Report and Security Review

Entities opt to use outside service organizations to process transactions as part of the entity's information system. Service organizations provide services ranging from performing a specific task under the direction of an entity to replacing entire business units or functions of the entity. When the operating activity is not directly administered by the entity, such as when utilizing a service organization, it is critical that appropriate monitoring controls are designed and implemented to reasonably ensure the service organization has adequate controls to achieve management's goals and objectives and complies with applicable laws and regulations. SOC-1 audits are performed over these service organizations to provide information about their internal controls to management and to auditors who rely on the SOC-1 report results for the audit of the entity's financial statements and IT systems.

RECOMMENDATIONS
(Continued)

The City Retirement System contracted with Levi, Ray, and Shoup (LRS) for a software hosting agreement including hosting, backup, technical assistance, system enhancement, and system updates of the Pension Gold application. The Retirement System also relied on the service organization's backup procedures and disaster recovery plan. However, a SOC-1 audit or internal security review was not completed for the Pension Gold applications that would provide the Retirement System with information about the effectiveness of the internal control over data processed at the service organization.

Without a SOC-1 audit, the Retirement System may not have sufficient information to reasonably ensure controls are in place to ensure the integrity of the data processed, maintained, and reported by the LRS software applications.

Future request for proposals and/or vendor contracts should include provisions for a SOC- 1 audit. The Retirement System should also take measures to ensure that the SOC-1 audit is completed for the LRS applications to provide the Retirement System and its auditors with a description of the system, results of the software application internal control testing, and an opinion of the overall processing environment.

4. Software support agreement

Successful software maintenance requires a software support agreement which addresses services provided, including support and training issues.

The City's software agreement for its Government Financial System (GFS) application had been amended, but included the original agreement signed in 1989. The City's approach to the software application has changed drastically since the original agreement when the City was involved in designed and modifying the application.

Lack of an updated, documented agreement could result in the City not receiving necessary services expected from its vendor.

The City should discuss with its vendor the need for an updated, documented support agreement. This agreement should include software upgrades, revisions necessary because of changes in law, provision for adequate training and user manual documentation, escrow of source code and other issues of concern to the City.

5. *Application Access Request Form: Government Financial System

Effective controls and District security policy require that network and application software user accounts be supported by an approved access request form.

For twenty two Government Financial System user accounts tested, six (27%) were not supported by an application access request form.

Lack of a documented access request form could lead to unintended access to application software, in which unauthorized users could cause malicious harm to the City information technology function.

A documented access request form should be required prior to granting application software access.

RECOMMENDATIONS
(Continued)

6. User Password Parameters

Users should be granted access to only those computer systems and functions they require to perform their job. To help ensure this, passwords are used to authenticate the identity of the user attempting to gain access to the computer systems. To prevent the integrity of these passwords from being compromised, passwords should have a password minimum length set.

The password maximum length for Tax is six characters, meaning it is possible to have a password of one character or blank. Per the City Information Security Policy, Version 3.0, June 2010, Section - 4.0 User Acknowledgements and Responsibilities: User passwords should be a minimum of 8 characters and must include at least one letter and one number, a special character is recommended.

Consistent with the City's security policy, all user accounts should be required to have a minimum password length of 8 characters. Additionally, the user access form should indicate the user's agreement with the City's policy.

* These matters were also reported in the audit of the 2013 financial statements.

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

Dave Yost
Auditor of State

Columbus, Ohio

February 26, 2015