



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 City of Cincinnati, Hamilton County, Ohio, (the City) in accordance with *Government Auditing Standards*, as of and for the year ended June 30, 2015, and have issued our report thereon dated January 29, 2016, wherein we noted the City adopted new accounting guidance in *Governmental Accounting Standards Board Statement No. 68, Accounting and Financial Reporting for Pensions – an amendment of GASB Statement No. 27* and *GASB Statement No. 71, Pension Transition for Contributions Made Subsequent to the Measurement Date - an amendment of GASB Statement No. 68*.

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 January 29, 2016, for the year ended June 30, 2015.

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 January 29, 2016, for the year ended June 30, 2015.

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.

Noncompliance Findings

1. ***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.

Twelve of forty-five (27%) of employee personnel files tested did not have a signed fraud reporting acknowledgement form.

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.

2. ***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 expenditures of federal awards (SEFA). However, for the Public Health Research fund (350) federal expenditures, we were unable to agree the amounts listed on the SEFA back to the City's general ledger or trial balance. We were able to agree these amounts to other supporting documentation.

The federal grant Shelter Plus Care has historically been reported under CFDA 14.238. In 2010 Congress updated the legislation, consolidating several programs into one. The regulations and appropriations from that point forward are authorized under CFDA 14.267, Continuum of Care. The City improperly reported this grant under 14.238 for all grant years on the SEFA. Failure to properly report federal expenditures can result in a loss of federal funding.

We also noted the following errors on the SEFA:

- CFDA 14.239: HOME outstanding loans should have been reported as \$37,748,495 instead of \$36,647,495 (\$1,101,000 difference).
- CFDA 14.218: CDBG NSP2 (\$197,552 in expenditures) and NSP3 (\$59,271) should have been reported under 14.256, Neighborhood Stabilization Program (Recovery Act Funded), due to these amounts being ARRA funded.
- CFDA 14.231: Emergency Solutions Grant (ESG) 2014 and 2015 should have been reported as \$544,080 and \$247,686 in expenditures, respectively, instead of \$462,257 and \$47,641, respectively, in order to agree to the trial balance (\$281,868 difference in total). Neither of the programs is material to the SEFA and neither is considered a major program.

- CFDA 93.224: Health Centers Cluster is listed as ARRA, but the grant agreement did not indicate this was ARRA funded (\$1,992,079 in expenditures).
- CFDA 16.922: Equitable Sharing Program should have been reported as \$373,646 in expenditures instead of \$37,646 in order to agree to the trial balance (\$336,000 difference). This difference is not considered material to the SEFA and this program is not considered a major program.

The City made the corrections to the SEFA. Failure to accurately account for separate 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 accurately account for separate federal funds in the City's general ledger.

3. **Ohio Rev. Code § 5705.10(I)**, states money paid into a fund must be used only for the purposes for which such fund has been established. The following funds had negative cash fund balances at June 30, 2015: Fund 304 - Community Development Block Grant of \$1,066,186; Fund 387 - Lead Hazard Control Research Grant of \$58,250; Fund 410 - Shelter Plus Care Program of \$8,367; Fund 436 - Environmental Studies of \$14,971; Fund 445 - Emergency Shelter of \$511,621; Fund 465 - Disaster Recovery Grant of \$317,461; and Fund 704 - MSD Capital Improvements of \$219,720.

A negative cash fund balance indicates that money from one fund was used to cover the expenses of another fund. We recommend that management monitor expenditures and available resources to avoid negative fund balances.

4. **The A-102 Common Rule and OMB Circular A-110** require that equipment be used in the program for which it was acquired or, when appropriate, other Federal programs. Equipment records shall be maintained, a physical inventory of equipment shall be taken at least once every 2 years and reconciled to the equipment records, an appropriate control system shall be used to safeguard equipment, and equipment shall be adequately maintained.

No physical inventory of equipment purchased with Federal funds has taken place in the last 2 years and reconciled to the equipment records for the Health Center Cluster Program. The grant coordinator did not know when the last inventory had been performed. Failure to comply with Federal requirements could result in the loss of Federal awards for the City.

We recommend a physical inventory of equipment be taken at least once every 2 years as required by the Federal awarding agency.

5. **OMB Circular A100 2 CFR 215 § 215.13** states Federal awarding agencies and recipients shall comply with Federal agency regulations implementing E.O.s 12549 and 12689, "Debarment and Suspension." Under those regulations, certain parties who are debarred, suspended or otherwise excluded may not be participants or principals in Federal assistance awards and subawards, and in certain contracts under those awards and subawards.

For the Continuum of Care grant, the City was not able to provide evidence that it had checked the vendors in 2 of 3 cases selected for testing to see whether they had been debarred. For the Transportation Investment Generating Economic Recovery (TIGER) Discretionary Grant Program

(TIGER), the City was not able to provide evidence that it had checked the vendors in 6 of 6 cases selected for testing to see whether they had been debarred.

If the City does not check the debarment list to see whether a potential vendor is on it, the City may do business with vendors that have been debarred, which is a violation of the above regulation. The City should check each vendor to see whether it is on the federal debarment list prior to paying grant money to that entity and should keep evidence of this check in its files..

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.

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. Network Policies

Network security parameters should be configured to require an authentication process for user login based on passwords which expire at a fixed interval and are not easily guessable. Certain aspects of network security were not consistent with industry standards.

Lack of appropriate authentication parameters according to industry standards weakens logical network security and exposes the network to greater potential for unauthorized access.

Password security parameters should be configured to restrict access to the network by requiring:

- Forced password expirations of at least 90 days for all users.
- Minimum password age of at least one day to prevent users from cycling through old passwords.
- Password history of at least four passwords in conjunction with a minimum password age, thereby preventing a user from simply reusing an old password upon its expiration for at least four password life cycles.
- Password complexity requirements to prevent users from using common words or all letters in their password.
- Minimum password length of at least six characters

Accounts should be locked out after three bad logon attempts, thereby requiring the network administrator to verify authenticity of accounts before resetting them.

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.

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.

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.

7. Employee Separation: Cincinnati Financial System (CFS) and CHRIS Applications

Proper computer security requires that user accounts be disabled or removed from the system upon employee separation.

Three former employees had application access privileges for the CFS application subsequent to separation of employment. For the CHRIS application, eighteen users had access rights but such employees were not reflected in the City's employee roster.

Departments are responsible for notifying the ETS staff upon employee separation. The Enterprise Technology Solutions (ETS) utilized a termination checklist for removing access rights to systems and applications upon termination. The form is required by ETS, while other departments are encouraged to use the termination checklist. Because the City employs 6,400 employees, some of which are part-time, without an automated procedure, it is possible the ETS department will not be notified in a timely manner regarding an employee separation.

The City should consider devising an automated procedure for notifying ETS upon employment separation to help ensure access privileges of those no longer with the City are immediately removed or disabled from the system. In addition, management should periodically review user accounts and their privileges to help ensure access rights are consistent with assigned job responsibilities.

8. Program Change Control

Effective program change practices include the use of a standard form to document authorization of requests for programming changes. Changes should be tested in a test library and documentation should be kept with the change request form or within the program code. Programmers should not have access to the production environment and a verification process should be in place to ensure the changes made are the changes moved into production.

The City has an informal process to request program changes. Testing is also done informally and usually documented within e-mail correspondence. A formal process is not in place to ensure that only the changes requested are the changes that are moved into production.

Without proper change control procedures, changes made to application software cannot be properly tracked to reference to if other changes to that program change need to be made. In addition, there is an increased risk these changes could go undetected and not be the proper change intended by management.

A formal process should be implemented that would include at a minimum:

- User requesting the change.
- Supervisor approval.
- Description of the change requested.
- Description of the changes made.
- Programmer who made the change.
- Test documentation.
- User approval of the changes made.
- Document and verify the change made is the change that is moved into production.

9. Continuum of Care (COC) Eligibility

The COC program provides rental assistance to tenants based on income amounts. We noted that 3 of the 60 tenants (5%) selected for testing did not have documentation of income in their file. All

of the files with missing documentation were for Talbert House clients. Failure to maintain documentation of income amounts could result in miscalculation of payment amounts available to the tenant.

The City should maintain income documentation in tenant files and implement procedures to improve the recordkeeping process at Talbert House.

10. Capital Assets

City management is responsible for preparing and fairly presenting their financial statements in accordance with accounting principles generally accepted in the United States of America; this includes designing, implementing, and maintaining internal controls relevant to preparing and fairly presenting financial statements that are free from material misstatement, whether due to fraud or error.

We noted the following conditions related to the City's record of capital assets:

- The City's CAFR did not agree to the City's fixed asset records due to the Mountain Square Plaza asset of \$20,076,747 not being included in Improvements in the City's capital asset listing, but properly included on the CAFR.
- The City made an improper reclassification from Improvements to Infrastructure in the amount of \$20,077,080. This reclassification was not approved by a supervisor.
- The City had projects recorded as Construction in Progress (CIP), which have not had any activity in at least two years. Failure to properly record construction in progress misstates the depreciable assets.

Lack of internal controls over accounting and financial reporting increases the risk that errors, theft or fraud could occur and not be detected in a timely manner. Failure to accurately post financial activity can lead to material misstatements in financial reporting.

We recommend that the City exercise due care when posting entries to the financial records and financial statement preparation to prevent errors and assist in properly reflecting the City's financial activity in the financial statements and properly disclose all activities of the financial statements as required. We also recommend that the City reconcile the capital asset amounts reported in the financial statements to make sure that all additions or deletions are also properly reflected in the capital asset listing. The City should ensure that all changes to assets are properly approved by a supervisor.

11. Investment Management Services

The City has contracted with Nuveen Asset Management, LLC and Bond-Tech, Inc. for investment management services. The City has not established procedures to determine whether the service organization has sufficient controls in place, which are operating effectively, to reduce the risk that securities have not been purchased or sold in accordance with the contract and City guidelines.

We recommend the City ensure securities have been purchased or sold in accordance with the contract and City guidelines. Furthermore, we recommend the City specify in its contract with the third-party investment manager that an annual SSAE 16/SOC 1 audit be performed. The City

should be provided a copy of the SSAE 16/SOC 1 audit report timely and should review the report's content. A SSAE 16/SOC 1 audit should be conducted in accordance with American Institute of Certified Public Accountants' (AICPA) standards by a firm registered and considered in "good standing" with the Accountancy Board of the respective State. If the third-party investment manager refuses to provide a SSAE 16/SOC 1 audit report, we recommend the City only contract with a third-party investment manager that will provide such a report.

12. Park Board Record Retention Schedule

The Forms RC-4 list the retention schedules for each of the City's departments, offices, boards and commissions. Each department, office, board, and commission request schedules based on the type of record and length of time the record(s) are needed to document their functions. The Park Board's retention schedule did not provide policy related to electronic records. We recommend the Park Board update its retention schedule to include electronic records. The Park Board is currently in the process of updating its retention schedule to include electronic records but the form RC-4 is in draft form and not yet approved by the City Records Commission.

* These matters were also reported in the audit of the 2014 financial statements.

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

Dave Yost
Auditor of State
Columbus, Ohio

January 29, 2016

DRAFT
CONFIDENTIAL