Dave Yost • Auditor of State

MANAGEMENT LETTER

City of Shelby
Richland County
43 West Main Street
Shelby, Ohio 44875

To the City Council:

We have audited the financial statements of the City of Shelby, Richland County, Ohio, (the City) in accordance with *Government Auditing Standards*, as of and for the year ended December 31, 2015, and have issued our report thereon dated November 15, 2016, wherein we noted the City adopted Governmental Accounting Standards Board (GASB) Statement No. 68, *Accounting and Financial Reporting for Pensions – an amendment of GASB Statement No. 27* and also GASB Statement No. 71, *Pension Transition for Contributions Made Subsequent to the Measurement Date*.

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 November 15, 2016 for the year ended December 31, 2015.

In addition to the matter communicated to you in the report described above, 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* report. 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.

NON-COMPLIANCE FINDING

1. Timely Depositing

Ohio Rev. Code § 9.38 states a person who is a public official other than a state officer, employee, or agent shall deposit all public moneys received by that person with the treasurer of the public office or properly designated depository on the business day next following the day of receipt, if the total amount of such moneys received exceeds one thousand dollars. If the total amount of the public moneys so received does not exceed one thousand dollars, the person shall deposit the moneys on the business day next following the day of receipt, unless the public office of which that person is a public official adopts a policy permitting a different time period, not to exceed three business days next following the day of receipt, for making such deposits, and the person is able to safeguard the moneys until such time as the moneys are deposited. The policy shall include provisions and procedures to safeguard the public moneys until they are deposited.

NON-COMPLIANCE FINDING (Continued)

1. Timely Depositing (Continued)

During our tests of utility receipts, we noted 64% (35 out of 55 days selected) were not timely deposited with the Finance Director by the business day next following the day of receipt. Failure to deposit receipts timely increases the risk of City funds being lost, misappropriated or improperly posted and these errors going undetected by management.

We recommend the utility department develop procedures to ensure all receipts are deposited with the Finance Director by the business day next following the day of receipt.

RECOMMENDATIONS

1. IT – Application Security Administration (Income Tax System)

User authentication is critical to help ensure computer resources are protected. Passwords are typically used to authenticate a user before access is granted to the computer system. Password expiration intervals are key components in helping to ensure only authorized individuals have knowledge of their user account name and password.

The City's finance department has established procedures that require user authentication through password protected user accounts. Although the Municipal Income Tax Solutions (MITS) application requires the submission of a valid username and password in order to access the application; passwords are not periodically changed. In addition, both municipal tax clerks in the Finance department know the username and password of the other tax clerk.

The risk of unauthorized access to critical resources through password disclosure increases when password change intervals are not established. In addition, individual accountability cannot be maintained when more than one person is aware of the username and password of an active account.

The City's finance department should implement password change controls for the MITS system, and discourage its users from sharing usernames and passwords to permit individual accountability of its user base and improve overall application security.

2. IT – Password Change – Municipal Court

Organizations restrict access to their computer systems, programs, and data to help reduce the risk of unauthorized access. Typically, logical access to automated information is restricted by the use of a password associated with access rules. Standard guidelines for password administration suggest implementing parameters over password length, complexity, history, and expiration. In addition, a periodic confirmation of user accounts should be performed to help ensure access has been granted to only those individuals who require access to perform their job duties.

Access to the Municipal Court's system is restricted with the use of password protected user accounts; however, the following weaknesses were noted:

- Account passwords are not set to expire.
- Two former employee accounts remained active on the system.
- Two accounts are maintained for the one staff member while only one account is necessary for this staff member's job function.

RECOMMENDATIONS (Continued)

2. IT – Password Change – Municipal Court (Continued)

The risk of unauthorized access to critical resources through password disclosure increases when password change intervals are not established. The presence of unused accounts also provides additionally avenues of attack that may not be adequately monitored. These conditions could result in an unauthorized individual gaining access to the system and accidentally or intentionally deleting or altering sensitive or financial data.

The Municipal Court should implement strong password change controls. Passwords should expire at least every 90 days for normal users and every 30 days for administrative accounts. In addition, a review of all user accounts on the system should be performed at least once a year to ensure access rights are appropriate and inactive accounts are removed timely.

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

Dave Yost
Auditor of State
Columbus, Ohio

November 15, 2016