

BlumShapiro

To the Members of the City Council and Management
City of New London, Connecticut

In planning and performing our audit of the financial statements of the City of New London, Connecticut, as of and for the year ended June 30, 2007 in accordance with auditing standards generally accepted in the United States of America, we considered the City of New London, Connecticut's internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the City of New London, Connecticut's internal control. Accordingly, we do not express an opinion on the effectiveness of the City of New London, Connecticut's internal control.

We noted the following matters involving the internal control over financial reporting and its operation that we offer as constructive suggestions for your consideration as part of the ongoing process of modifying and improving accounting controls and administrative practices.

ACCOUNTING AND GENERAL MATTERS

PRIOR YEAR'S ITEMS UNRESOLVED

In the prior year, we noted some items which have not been resolved as of the date of this letter. These items have been elevated from control deficiencies to significant deficiencies and/or material weaknesses. The items can be found in our letter dated July 14, 2008 as items #2007-01 and 2007-04.

CURRENT YEAR ITEMS

Compensated Absences

During our audit, we noted that compensated absences were incorrectly calculated when originally received and also not performed timely.

Recommendation - We recommend that all sick, vacation and compensated time should be summarized on a monthly basis and calculated annually in a timely manner for audit purposes.

Cafeteria Fund

During our audit, we noted that the Cafeteria Fund financial statement was not completed accurately or timely.

Recommendation - We recommend that cafeteria fund activity be recorded on a monthly basis and summarized annually for audit purposes.

Board of Education General Journal Entries

During our audit, we noted that proper documentation was not kept to support the general journal entries. While documentation was eventually obtained, it was a very cumbersome process.

Recommendation - We recommend that the proper supporting documentation be kept with all general journal entries in order to support the amounts in the books and records of the Board Of Education. Care should be taken to preserve the financial records of the City.

TECHNOLOGY SECURITY MATTERS

In support of the financial audit, Blum Shapiro Consulting performed an IT general controls review of the information technology function for the City and the BOE during the fiscal year ended June 30, 2005. The findings and recommendations that have not yet been implemented are summarized below together with the current year status:

1. Windows NT/2000/2003 User ID and Password Controls Need Improvement

Although user IDs and passwords are used to access the City's network, their effectiveness is impacted by the lack of key controls; specifically, users are not forced to periodically change their passwords.

The continued use of the same password severely diminishes the usefulness of passwords. Without regular changes, the opportunities for abuse increase dramatically. Most network operating systems, including Windows NT/2000/2003, provide a means that automatically forces users to change their passwords within a defined time period (60 to 90 days is typical).

Recommendation - Implement Additional User ID Access Controls

Network operating systems allow for many different levels of user access controls through a variety of unique parameters. We recommend that the City of New London establish a regularly forced password change to occur every 60 or 90 days requiring all staff to create a new, unique password for their ID. We also recommend that users be required to create a different password at each interval change.

All passwords for administrative or supervisory IDs for all network operating systems should also change on a 60 to 90 day basis. Each password should also be unique to limit potential unauthorized access to network resources at a very sensitive level.

User IDs should also be locked after three unsuccessful attempts and require the system administrator to reset the ID. This approach should raise the awareness of any unauthorized attempts to access the City's network by someone outside of the City.

Due to the critical nature of financial information within the City, all Windows 98/NT/2000/XP PCs should be password protected and "locked down." This means that

users must log into their respective PC, not be allowed to load new software, not be allowed to modify PC configurations, and password protected screen savers be implemented after a specific period of time. This will enhance PC desktop security and minimize the ability for “outsiders” to access sensitive financial information.

Current Year Status: The City has partially implemented this recommendation. The IT department feels it would be difficult to fully implement. The BOE implemented this recommendation.

2. Information Systems Policies and Procedures Are Not Enforced

The City does not completely enforce the Computer Systems and Internet Usage Policy. In particular, during the interview process, it was confirmed that there are some users who share user IDs and passwords. Specific policies and procedures need to be enforced to secure the City’s network and provide direction to staff regarding the appropriate and acceptable use of network systems

Recommendation - Enforce the Technology and Operational Policies and Procedures

The City needs to re-introduce and formalize the current set of standard policies and procedures in order to secure and protect its technology infrastructure. In addition, employees should be forced to again sign off on these policies, confirming that they have read and will abide by them. After sign off, violation of the policies and procedures should be grounds for formal warnings and/or termination.

Current Year Status: The City implemented this recommendation. The BOE distributes a technology handbook but does not require employee signoff showing receipt of these policies and procedures.

3. Data Backup Tapes Are Not Regularly Tested

The tapes used as part of the City’s regular data backup procedure are not regularly tested to ensure that information is successfully being recorded on the tapes used. The City does review daily backup logs but does not periodically attempt to restore a test file from random tapes to ensure that the entire backup and recovery process functions as anticipated. As a result, in the event of an emergency, the City may not be able to restore critical files when needed most.

Recommendation - Perform Regular Tests of Data Backup Media

The City should introduce into its backup procedure a regular monthly/quarterly test of the backup tapes. Staff should attempt to recover a test data file from a randomly selected tape. This will allow the City to confirm that the process, tapes and tape drive are working as required and will function when needed.

Current Year Status: The City has not yet fully implemented this recommendation. The BOE implemented this recommendation.

4. A Documented Disaster Recovery Plan Does Not Exist

The City does not have a documented plan to ensure the quick and orderly recovery of business operations in the event of an emergency. Although staff may have a “reasonable” idea of what is required to restore critical business systems in a timely fashion, it will be difficult to ensure all aspects of the City’s network and computer services are addressed during a time of crisis. A documented plan will provide both IT and City management with the information necessary to ensure all activities are addressed, required hardware and software are identified and appropriated, and task responsibilities are assigned to appropriate key personnel.

Recommendation - Develop and Test a Comprehensive Disaster Recovery Plan

A documented Disaster Recovery Plan should be developed to provide a “roadmap” of key activities and responsibilities for staff in the event of an emergency. This plan should include, at a minimum:

- a. Prioritization of systems for recovery
- b. Assignment of staff roles and responsibilities
- c. Inventory of systems and data maintained on the various servers
- d. Hardware, operating system and application configuration data
- e. Vendor contacts for mission critical systems
- f. Location of backup media and software
- g. Potential off-site recovery locations

Once developed, this plan should be tested on a regularly scheduled basis to confirm that procedures are still applicable to the current technology environment. We also recommend that a copy of the plan be maintained off-site with the system backup software and the daily and/or monthly backup tapes to ensure all key elements are available and accessible.

Current Year Status: The City and BOE have not yet implemented this recommendation.

5. Staff Hiring/Termination Controls Are Not Effectively Applied

The procedures used to notify the IT Department of when new staff is hired or, conversely, when staff is terminated, are not consistently followed to ensure proper controls are maintained over the City’s technology environment. When a City employee is terminated, the IT Department is not informed on a timely basis to disable the employee’s network access, leaving the account active and accessible. As a result, the City’s network is open to potential abuse by the departing employee or others who may know the employee’s password.

Recommendation - Implement Stronger Hiring/Termination Notification Procedures

The City needs to implement procedures that ensure the IT Department is given sufficient notice of any hiring or termination actions that will affect the City's network security. At a minimum, the IT Department should be notified by electronic mail that a user account needs to be created or disabled so that a documented record is maintained. For new hires, this notice should provide the necessary information for creating a user account with the access rights appropriate to the new employee's position. In termination situations, the City should give the IT Department necessary notice to disable the employee's account in order to minimize potential damage to the City's data and computing resources. All notifications should come from an authorized source to ensure only appropriate actions are taken.

Current Year Status: The City has not yet implemented this recommendation. The BOE implemented this recommendation.

This letter should be read in conjunction with our report on Internal Control over Financial Reporting and on Compliance Based on an Audit of Financial Statements Performed in Accordance with *Government Auditing Standards* dated July 14, 2008.

This communication is intended solely for the information and use of management, the Members of the City Council, the Board of Finance, others within the City and federal and state awarding agencies and pass-through entities and is not intended to be and should not be used by anyone other than these specified parties.

Blum, Shapiro & Company, P.C.

July 14, 2008