Mayer Hoffman McCann P.C.
An Independent CPA Firm

2301 Dupont Drive, Suite 200
Irvine, California 92612
949-474-2020 ph
949-263-5520 fx
www.mhm-pc.com

City Council

City of Pasadena
Pasadena, California

In planning and performing our audit of the financial statements of the City of Pasadena (City) as of and for the year ended June 30, 2010, in accordance with auditing standards generally accepted in the United States of America, we considered the City's internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the City's internal control. Accordingly, we do not express an opinion on the effectiveness of the City's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be deficiencies, significant deficiencies, or material weaknesses and therefore there can be no assurance that all such deficiencies have been identified.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. **We did not identify any deficiencies in internal control that we consider to be material weaknesses.**

A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. The matters below described as items 10-01 and 09-01 conform to this definition.

(10-01)   Need to Improve Control over Paramedic Billing and Collections

> During our review of the accounts receivable, we noted that the recorded Paramedic Receivables as of June 30, 2010 were over $7 million with allowance for doubtful account calculated as 50% of the receivable amount. Fiscal Year 2010 is the first year that the City contracted a third party to perform billing and collection for Paramedic receivables. There was no yearend accounts receivable aged report that was presented

for audit purposes because the City is unable to obtain such report from its contractor. We reviewed the report that the City obtained from the contractor which shows a summary of monthly billing amounts and collections and noted that there is a column for "Unbilled and Write Off" that amounted to over $1 million. Per our inquiry with City personnel, this amount represents amounts that are not billed pending additional information to complete the billing. As a best practice, a year end aging report should be periodically reviewed for old and slow-paying accounts. Additionally, the City should be able to obtain a detail of the unbilled and write off balance to be reviewed and ensure that there haven't been any write-offs not unauthorized by the City.

Recommendation

We recommend that the City continue their effort in working together with the contractor to improve control over billing and collection of the Paramedic Receivable.

Management's Comments Regarding Corrective Actions Planned

Management concurs with the auditors recommendations. As commented on above, the outside vendor was unable to provide a detailed accounts receivable aging at year end. Subsequently such a report has been received and staff is carefully reviewing and will implement further actions to validate the vendor data and improve the timely receipt of proper documentation from the vendor.

As a service to you, we also identified during our audit certain matters that provide you an opportunity to enhance your existing internal controls. These matters are provided as recommendations for your consideration and are not considered to be material weaknesses in internal or significant deficiencies in internal control:

10-02   Develop an IT Strategic Plan

During our review of Information Technology (IT) General Controls we noted the City does not have an IT Strategic Plan. IT strategic planning is a significant step for aligning IT resources with the business strategy and priorities. An IT strategic plan defines, in co-operation with relevant stakeholders (personnel affected by strategic planning), how IT goals will contribute to the City's strategic objectives and related costs and risks. The plan should:
• Improve key stakeholders' understanding of IT opportunities and limitations, assesses current performance, identifies capacity and human resource requirements, and clarifies the level of investments required.

- Include how IT will support IT-enabled investment programs, IT services and IT assets.
- Define how the objectives will be met, the measurements to be used and the procedures to obtain formal sign-off from the stakeholders.
- Cover investment / operational budgets, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements.

Without appropriate strategic planning, the City will not be able to maximize the potential to build a better relationship between management and their users or between the City and their citizens.

Recommendation

We recommend the City develop and implement an IT Strategic Plan.

Management's Comments Regarding Corrective Actions Planned

The City of Pasadena is already underway with the development of a comprehensive IT Strategic Plan. The City is committed to the effective use of the City's IT investment while implementing new technology to ensure the efficient and effective delivery of City services to our community. In order to maximize the return on investment in technology and minimize duplication, the City of Pasadena is in the process of creating a comprehensive IT Strategic Plan for technology advancements which meets the goals, objectives and vision of the community and our organization. The IT Strategic Plan will be completed in February, 2011.

10-03 Enhancing Security Controls Over Information Technology Systems

During our review of user access controls and password settings for users logging onto the City's internal network, we noted that certain security policies and procedures could be enhanced to provide better security over the City's network and application processing environment.

1. The default domain password settings are set to the following specifications:
   - Minimum Password Length – 6
   - Password Change Interval – 180 days.
   - Password Complexity – Disabled
   - Password History Remembered – 3 passwords
   - Account Lockout Threshold – 50 attempts

For increased security over system resources, industry best practice recommends the following default domain password settings:

- Minimum Password Length – 8
- Password Change Interval – 90 days or less.
- Password Complexity – Enabled
- Password History Remembered – 4 passwords (or at least 1 year when used in conjunction with the Password Change Interval)
- Account Lockout Threshold – 3-5 attempts

Password complexity requirements typical force user passwords to include at least 2 of the following:
a. uppercase character,
b. number, and
c. special character.

2. A sample of 25 terminated users were selected for testing to ensure their access to City resources were removed. We noted the following during testing:
- 5 of 25 terminated users have active network accounts.
- 6 of 25 terminated users have active financial system accounts.
- 4 of 25 terminated users have active remote access accounts.

Access controls limit or detect inappropriate access to computer resources, thereby protecting them from unauthorized modification, loss, and disclosure. Logical access controls require users to authenticate themselves (through the use of secret passwords or other identifiers) and limit the files and other resources that authenticated users can access and the actions that they can execute. Our testing of logical access controls included a review of policies and procedures, organizational structure, access control lists, and password settings.

Without adequate access controls, unauthorized individuals, including outside intruders and former employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. In addition, authorized users can intentionally or unintentionally read, add, delete, modify, or execute changes that are outside their span of authority. Inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data.

Recommendations

We recommend the City:
1. Enhance password controls to better align with industry best practice.
2. Enhance internal controls to ensure terminated users logical and physical access is removed timely following their termination date (i.e., within 1-3 business days).
3. Implement procedures to review user access on a periodic basis to ensure access is current and appropriate. The review should also be used to determine appropriate segregation of duties for users of financial software.

Management's Comments Regarding Corrective Actions Planned

The Department of IT has developed password policies around industry standard and best practices. Those policies continue to be adopted in the organization.

Standard account terminations are currently handled through Entry/Exit and a process exists for account termination for more sensitive situations. Additionally a yearly audit is performed for active user accounts per department.

Periodic user access auditing is a process we are looking to implement in the future, as part of the reorganizing of roles and responsibilities within the Department of IT. The department of IT has a documented and enforced policy of "least privilege", which has been in place for three years. This policy means that IT only grants permissions to what is required to do the job. Additionally we have implemented "role based access" creating permissions based on a user's role only. Auditing is reviewed for log on and off events, on a requested basis and attempted password changes, both successful and unsuccessful are reported automatically to IT and the user whose password has been attempted to be changed. In the future efforts are being made to develop and maintain audit log review by the application or data owners.

10-04 Security Awareness Training

During our review of IT procedures and controls, we noted that security awareness training is not provided to employees and contractors of the City.

Effective security-related personnel policies are critical to effective security. Ineffective personnel policies can result in employees or contractors inadvertently or intentionally compromising security. For example, security may be compromised due to an inadequate

awareness or understanding, inadequate security training, or inadequate screening of employees. An ongoing security awareness program should be implemented that includes first-time training for all new employees, contractors, and users; periodic refresher training for all employees, contractors and users; and distribution of security policies detailing rules and expected behaviors to all affected personnel.

Recommendation

We recommend that an ongoing security awareness program be implemented. Relevant security awareness requirements and guidance can be found in are contained in the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) Circular A-130, and the National Institute of Standards and Technology (NIST) SP 800-50, *Building an Information Technology Security Awareness and Training Program*. In addition, employees with significant security responsibilities should receive specialized training, as described in NIST SP 800-16, *"Information Technology Security Training Requirements: A Role and Performance-Based Model"* (April 1998).

Management's Comments Regarding Corrective Actions Planned

Security training is part of an overall objective towards the goal of City of Pasadena security awareness. In addition to training, awareness is achieved through security policies, standards and procedures. Formal training is a role that will be performed by the City IT Security Officer, which is a new position identified and recommended as part of the IT Audit and upcoming IT Strategic Plan.

10-05   Improve Environmental Controls and Develop Contingency Plans

During our discussion with management it was noted there is no contingency plan to deal with short or long term contingencies. In addition, it was noted that there is no power generator to provide long term power in the event of an extended power outage and no plans for a backup recovery facility.

Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect the City's ability to accomplish its mission. If contingency planning controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information.

Controls to ensure service continuity should address the entire range of potential disruptions. These may include relatively minor interruptions, such as temporary power failures, as well as major disasters, such as fires, natural disasters, and terrorism, that would require reestablishing operations at a remote location. If controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data. To mitigate service interruptions, it is essential that the related controls be understood and supported by management and staff throughout the City. Senior management commitment is especially important to ensuring that adequate resources are devoted to emergency planning, training, and related testing. Also, the involvement of data and process owners is integral to contingency planning, as they have first-hand knowledge of their data and processes and of the impact of a loss of availability.

Recommendations

We recommend the City develop and document a comprehensive contingency plan that takes into account both short and long term contingencies. The plan should include possible solutions for providing ongoing power to the primary computer room in the event of an extended power outage. In addition, we recommend the City designate a backup computer room at a remote facility to be used in the event the primary computer room is no longer available. In the event using a specialized third party recovery facility is too expensive, we recommend contacting other local governments to determine if they have the capability to house computer equipment in their computer room in the event of a contingency as part of a reciprocal agreement.

Management's Comments Regarding Corrective Actions Planned

The Department of IT has identified the need to develop a City contingency and disaster recovery plan. This plan will be a priority project for the department over the next year. Currently the Department of IT performs backups of all city data, and they are sent offsite in case of a disaster. The package of data sent offsite includes application data, recovery steps, organizational documentation, passwords, vendor contacts and more.

Environment controls and contingency plans continue to be an active area that the Department of IT is working towards. The department has explored becoming a recovery site partner with other cities, and has initial plans to use one of the City's four datacenters as a potential mirror or recovery site. Two of the four datacenters managed by the City have full-time generators. The department purchased a site recovery product and plans to implement the product in the near future at one or two of the City datacenters with full-time generators.

The primary datacenter has a generator hookup and has been successfully tested with a power cutover. The City of Pasadena owns several generators, which can be used in the event of a disaster and maintains an external generator service provider list. The department has investigated the possibility of a permanent generator, and options continue to be explored around making that investment.

STATUS OF PRIOR YEAR AUDIT FINDINGS

During the audit for the year ended June 30, 2010, we determined the status of prior year audit findings previously communicated to City Council. The original comments as well as the status of those comments are included in this report.

(09-1) Enhancing Controls over Supplies Inventory

The City has a formal policy regarding inventory cycle counts. Cycle counts are performed regularly in accordance with the policy, with a focus on high-value material items. During the audit of fiscal year ended June 30, 2009 results of the cycle counts performed were validated through our physical inventory observation, although it was noted that one high ticket item that had been withdrawn from inventory remained reflected as inventory in the City's accounting records. It is important to identify and remove withdrawn inventory from the accounting records in a timely manner.

Recommendation

We recommend that the City continue to improve policies and procedures to enhance proper accountability over inventory records and physical inventory counts.

Status

Not Resolved. During year ended June 30, 2010, the City's Internal Auditor conducted an audit on controls over inventory of supplies. The internal auditor observed a cycle count of switches on three days in June 2010 and the result indicated that eight switches may have been withdrawn from inventory but remained as inventory in the accounting records. As of year-end these switches could not be identified and the City's accounting records had to be adjusted accordingly.

Management's Comments Regarding Corrective Actions Planned

PWP staff concurs with the recommendation for continued improvement of policies and procedures to ensure proper accountability of inventory records. Field personnel have received additional instruction as to the proper procedures to follow when requisitioning material. However, there are circumstances under which complete requisition information is not available at the time material is needed. PWP field operations personnel are required to respond to emergency power interruptions or water main breaks, often after regular business hours when materials inventory staff is not available. PWP has enhanced materials requisition procedures for emergency responses and will continue to pursue utility industry best-practices for managing inventory requisitions while ensuring that timeliness for emergency responses remains a top priority.

Although eight electrical switches were identified during the physical inventory count that had been withdrawn from inventory but remained in inventory based on accounting records, five of those switches were later located and properly classified. Only three electrical switches were included in the adjustment of accounting records.

Beginning in July 2010, materials inventory staff has implemented a tracking system whereby all items for which a requisition has not been issued are tracked in a separate log that includes the item number and description of the material to be removed, along with the date and name of the crew supervisor responsible for removing the material. The log book is then reconciled with actual work orders and requisitions issued with any differences resolved over a two week period.

In addition, a fence has been installed around the materials inventory that does not require forklift relocation to improve security. The fence ensures that proper paperwork and procedures are followed before material is issued. Additional security cameras will also be installed throughout the materials storage area to provide additional security for materials and equipment.

(06-3) City Management Review of Skidata Reports Provided by Modern Parking

Modern Parking Inc. performs parking garage management services for the Paseo Colorado garages. The three parking garages of the Paseo Colorado Development include the Marengo Avenue Garage, the Subterranean Paseo Colorado Garage, and the Los Robles Avenue Garage. These three parking facilities provide transient and monthly parking for patrons, employees, and residents.

During our audit for the fiscal year ended June 30, 2006, we noted that the City of Pasadena received a Daily Deposits Report, which was an excel based report that summarized the cash receipts that were collected for each parking garage. At the end of each month the City also received a Garage Summary Report, which was an excel based report that summarized the parking revenue for the month. This report was used to record the parking revenue by garage and to reconcile the daily deposits per the Daily Deposits Report and the bank statement. However, the City did not receive any system generated reports from the parking garage's database. The parking garage is operated by a program called Skidata. Skidata tracks the time of entry and exit for each parking ticket, validations, and is integrated with the cashiering system.

Recommendation

We recommended that the City be provided a system generated report from Skidata at least monthly in order to compare the cash receipts reported on the monthly *Garage Summary Report* to actual parking activity per Skidata. This reconciliation will ensure that all cash receipts recorded in Skidata have been deposited.

Status

Partially resolved. Based on the results of testwork performed, we found that the Parking Division is provided system generated reports by Modern Parking. However, the reconciliation of the reports was not performed since December 2009.

Management's Comments Regarding Corrective Actions Planned
Management concurs with the auditors recommendations.

The written responses and comments provided by the City have not been subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on them.

This report is intended solely for the information and use of the City Council and management of the City of Pasadena and is not intended to be and should not be used by anyone other than these specified parties.

Mayer Hoffman McCann P.C.

Irvine, California
December 6, 2010