GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE INSPECTOR GENERAL

DISTRICT OF COLUMBIA MANAGEMENT RECOMMENDATIONS

FISCAL YEAR 2015

DANIEL W. LUCAS
INSPECTOR GENERAL

OIG NO. 16-1-13MA March 2016

Mission

The mission of the Office of the Inspector General (OIG) is to independently audit, inspect, and investigate matters pertaining to the District of Columbia government in order to:

- prevent and detect corruption, mismanagement, waste, fraud, and abuse;
- promote economy, efficiency, effectiveness, and accountability;
- inform stakeholders about issues relating to District administration and operations; and,
- recommend and track the implementation of corrective actions.

Vision

To be a world class Office of Inspector General that is customer-focused, and sets the standard for oversight excellence!

Report Fraud, Waste, Abuse, or Mismanagement

OIG

Email: hotline.oig@dc.gov

Telephone: (202) 724-TIPS (8477) or (800) 521-1639

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Inspector General

Inspector General

OIG

March 31, 2016

The Honorable Muriel Bowser
Mayor
District of Columbia
Mayor's Correspondence Unit, Suite 316
1350 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

Jeffrey S. DeWitt
Chief Financial Officer
Office of the Chief Financial Officer
John A. Wilson Building
1350 Pennsylvania Avenue, N.W., Suite 203
Washington, D.C. 20004

The Honorable Phil Mendelson
Chairman
Council of the District of Columbia
John A. Wilson Building
1350 Pennsylvania Avenue, N.W., Suite 504
Washington, D.C. 20004

Dear Mayor Bowser, Chairman Mendelson, and Mr. DeWitt:

Enclosed is the District of Columbia Management Recommendations report issued by SB & Company, LLC (SBC) for fiscal year 2015 (OIG No. 16-1-13MA). SBC submitted this report as part of our overall contract for the audit of the District of Columbia's general purpose financial statements for fiscal year 2015.

This report sets forth SBC's comments and recommendations intended to improve internal controls or result in other operating efficiencies in District Government. My office will conduct a follow-up on agency actions taken to address the conditions identified by SBC.

If you have any questions concerning this report, please contact me or Toayoa D. Aldridge, Assistant Inspector General for Audits, at (202) 727-2540.

Sincerely,

Daniel W. Lucas
Inspector General

DWL/mnw

Enclosure

cc: See Distribution List

DISTRIBUTION:

Mr. Rashad M. Young, City Administrator, Attention: Mr. Barry Kreiswirth (via email)
Ms. Brenda Donald, Deputy Mayor for Health and Human Services, District of Columbia (via email)
The Honorable Jack Evans, Chairperson, Committee on Finance and Revenue, Council of the District of Columbia (via email)
The Honorable Yvette Alexander, Chairperson, Committee on Health and Human Services, Council of the District of Columbia (via email)
Mr. John Falcicchio, Chief of Staff, Office of the Mayor (via email)
Mr. Michael Czin, Director, Office of Communications, (via email)
Mr. Matthew Brown, Director, Mayor's Office of Budget and Finance (via email)
Ms. Nyasha Smith, Secretary to the Council, Council of the District of Columbia (1 copy and via email)
Ms. Tracey H. Cohen, Interim Executive Director, D.C. Lottery and Charitable Games Control Board (via email)
Mr. Andrew L. Davis, Interim Chief Executive Officer, United Medical Center (via email)
Ms. Archana Vemulapalli, Acting Chief Technology Officer, Office of the Chief Technology Officer (via email)
Mr. Timothy Barry, Executive Director, Office of Integrity and Oversight, Office of the Chief Financial Officer (via email)
The Honorable Kathleen Patterson, D.C. Auditor, Office of the D.C. Auditor, Attention: Candace McCrae (via email)
Mr. Jed Ross, Director and Chief Risk Officer, Office of Risk Management (via email)
Mr. Graylin (Gray) Smith, Partner, SB and Company, LLC

The District of Columbia

Management Recommendations

For the Year Ended September 30, 2015

SB & COMPANY, LLC
KNOWLEDGE • QUALITY • CLIENT SERVICE

To the Mayor, City Council, Inspector General
and Chief Financial Officer of the District of Columbia

In planning and performing our audit of the basic financial statements of the District of Columbia and related entities (the District) as of and for the year ended September 30, 2015, in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, we considered the District's internal control over financial reporting (internal control) as a basis for designing audit procedures that were appropriate in the circumstances 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 District's internal control. Accordingly, we did not express an opinion on the effectiveness of the District's internal control over financial reporting.

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 significant deficiencies or material weaknesses and therefore, significant deficiencies or material weaknesses may exist that have not been identified. Although no matter of a material weakness was noted, other recommendations have been noted which we believe will further improve the District's internal controls or operating effectiveness.

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 a 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. None of the identified deficiencies in internal control were considered to be a material weakness.

This letter does not affect out report dated January 27, 2016, on the financial statements of the District. We will review the status of the comments during our next audit engagement. Our comments and recommendations, which have been discussed with appropriate members of management, are intended to improve the internal control or result in other operating improvements.

SB & COMPANY, LLC
KNOWLEDGE • QUALITY • CLIENT SERVICE

The purpose of this communication, which is an integral part of our audit, is to describe, for management and those charged with governance, our observations and recommendations to improve the District's internal controls and operations. Accordingly, this communication is not intended to be and should not be used for any other purpose.

Washington, DC
January 27, 2016

SB & Company, LLC

SB & COMPANY, LLC
KNOWLEDGE • QUALITY • CLIENT SERVICE

DISTRICT OF COLUMBIA

TABLE OF CONTENTS

GENERAL GOVERNMENT

DISTRICT OF COLUMBIA LOTTERY

NOT FOR PROFIT HOSPITAL CORPORATION

SB & COMPANY, LLC
KNOWLEDGE • QUALITY • CLIENT SERVICE

GENERAL GOVERNMENT

1. Remove Permissions to the Database Supporting the SOAR Financial Application

During our review of the permissions to the database supporting SOAR we noted the following:

- SOAR programmers have system administration permissions to the database that are not needed to complete their assigned job duties.
- A systemic report is not generated to provide visibility when changes are made with these permissions to the DB2 tables supporting SOAR to ensure that only authorized changes are made. Producing a system report of DB2 activity would allow for a reconciliation to be performed, to ensure that only authorized changes have been made.

Unauthorized changes could be made to the database which could impact the completeness and accuracy of financial data.

Recommendations:

We recommend that management remove permissions granted that are not needed to compete assigned job duties. We also recommend that a systemic report be put in place to alert management when changes are made to the database supporting SOAR.

Management Comments:

Management concurs with the principle that the least needed permissions should be assigned. Based upon feedback from the production Data Base Administration and production control, Management intends to test the removal of SYSADMAUTH from one user profile to confirm that removing this permission will not negatively impact the daily processing of batch jobs or impede production support. If no problems are identified, SYSADMAUTH will be removed from the other users.

Management will review the database permissions with the production support team to determine the appropriateness of these permissions and will revoke them if there is no justifiable need.

2. Improve Information Security Processes and Procedures Supporting the Office of the Chief Financial Officer

During our review of Information Security processes and procedures supporting the OCFO, we noted the following:

- Current processes do not ensure that access permissions to the server rooms are removed timely when individuals leave the OCFO.
- A secured configuration build guide is not currently in place for the operating system and the database supporting the iNovah application.

- Automated reports are not being generated to identify changes to database tables. Generation and review of such reports would allow for a reconciliation process designed to ensure that only authorized changes have been made.
- Testing of the Disaster Recovery Plan has not been performed to ensure necessary procedures can be executed to resume operations from a remote location in the event of a disaster.
- There is not a documented process for handling changes to the iNovah application.
- Currently, there is no documented Data Retention Policy in place to address the requirement timeframes for maintaining critical data.

Without the appropriate Information Technology processes and procedures in place, there is increased exposure to unauthorized activity which could cause technology resources to be unavailable, and therefore resulting in disruptions to government operations.

Recommendations:

- We recommend that active cards with access to the server rooms be re-evaluated and disabled if no longer needed or the level of access granted is not commensurate with assigned job duties.

- We also recommend that management develop a secure build for critical configuration of the OS and database supporting iNovah and perform periodic reviews of critical configuration parameters to verify compliance with secured configuration requirements.

- Management should also generate systemic reports to identify changes to the SQL database supporting iNovah. The changes per the report should be reconciled to the approved change request form(s).

- In addition, management should perform periodic Disaster Recovery testing to verify that critical data and applications can be restored from a remote location. Formal documentation should be in place for the restore testing process.

- We further recommend that management document the change management process and develop a Data Retention Policy which should include retention procedures and timeframes.

Management Comments:

Management will disable access for two employees that have recently left the District employment. It is important to note that their cards have been collected and therefore their access is effectively disabled. Management performs a quarterly review of access rights. The next review is scheduled for January 2016. Users with no accepted justification for access will be disabled.

Management concurs that documentation on the secure build for the servers and database supporting financial data should be maintained and that an annual review of the server to confirm it conforms to the secure build should be conducted.

Management concurs that audit tracking on the iNovah database should be enabled. Management will conduct a review of the audit report on a quarterly basis.

Management concurs that an annual Disaster Recovery test for critical applications and systems housed in the Office of the Chief Information Officer (OCIO) server room should be conducted. Management has directed that each system have its own recovery plan documented and approved in FY 2016 and that a Business Continuity plan for the OCFO be developed to provide for remote operations in the event of a disaster.

Management has begun to improve the current change management review process and intends to augment it in Fiscal Year 2016 to ensure that all production application changes are included in the revised CCB process.

Management agrees that a formal policy defining retention procedures and periods will be developed for iNovah and other business critical applications for which a policy is not yet formally in place.

3. Define and Evaluate Logical Permissions for the Database Supporting SOAR Database

The SOAR application relies on the DB2 database to support the application. The data and critical calculations for these applications normally reside in the DB2 tables.

Our review of logical access for Information Security and System Administration to the DB2 environment indicated that the System Administration and Information Security Administration's logical permissions have not been separated for the DB2 environment. Also systemic reports are not produced of changes made by the DB2 System Administrators.

As a result, unauthorized activity which could lead to inaccurate financial reporting may not be timely detected.

Recommendation:

We recommend that management logically define the DB2 environment to separate DB2 System Administration and Information Security functions. Management should also evaluate the feasibility of strategically moving to Resource Access Control Facility to manage privileges to DB2. We further recommend that management implement reports that will automatically generate to alert management when changes are made to the DB2 environment.

Management Comments:

Management concurs that "Information Security and System Administration permissions to the SOAR Production DB2 environment are not currently separated." Management will determine, from a business, operational, and cost perspective, the implications of separating the duties and, unless there is a strong reason not to separate the duties, implement the separation of duties.

Management will evaluate the practicability of using external security, namely, RACF, to manage the privileges of the SOAR Production DB2 environment.

Management concurs with the statement that, "Reports are not in place for agencies to receive when changes have been made to DB2 tables supporting agency application." Minimally, OCTO will implement auditing for Production SOAR as was done for Office of Tax and Revenue per the Internal Revenue Service. If possible, we will audit everything done within DB2 by System Administrators. Beyond that, OCTO requires more specificity. For example, more information is needed regarding the tables considered to be critical.

4. Reevaluate Network Security Supporting the Office of Chief the Financial Officer (OCFO)

The following concerns were identified during the review of network security:

- The firewall rules need to be re-evaluated and refined to allow only traffic needed to support business operations. There were rules open in the firewall that allowed excessive traffic inbound.

- Data Loss Prevention (DLP) software is not currently in place. DLP software can detect and prevent unauthorized attempts to send data outside of the DC network.

Without adequate network security support, there is increased risk exposure to external threat.

Recommendations:

We recommend that the Office of Chief the Financial Officer and DCLB perform re-evaluation of firewall rules and refine rules where needed. We also recommend that management review redundant IPS to prevent traffic not being inspected that should be installed. We recommend that DLP software should be implemented to prevent data theft should be put in place.

Management Comments:

Management agrees that the firewall rules should be re-evaluated and refined in light of concerns raised on limiting traffic to support business operations. Management agrees that a back-up or fail-over IPS device needs to be installed at Lottery and Charitable Games Control Board to ensure business continuity. Management agrees that DLP software should be added to the Office of Chief the Financial Officer domain and shall engage Office of the Chief Technology Officer in a discussion on how to manage DLP on the DC network.

DISTRICT OF COLUMBIA LOTTERY

5. Deficiency in Information Security Processes — Information Security Processes and Procedures Supporting DC Lottery

Review of Information Security processes and procedures supporting the DC Lottery technology platforms indicated the following concerns:

- The entitlement review process currently performed does not capture all of the accounts related to the ICS application, Windows Operating System, Oracle database and the Data Center.

- The review of the configuration management processes for the Windows server and Oracle database supporting DC Lottery disclosed the following:

- A secured build guide is not in place for the operating system and database supporting the financial application ICS.

- Currently, there are no procedures for a periodic review of configuration baselines for the operating system and database supporting the DC Lottery financial application.

- Review of the Oracle supporting the ICS data disclosed the following concerns:

- A formal process and related procedures have not been put in place to monitor and account for the use of Oracle's high privileged accounts.

- Profile settings for password controls are not currently enabled for the Oracle database.

- Systemic reports are not generated to identify changes made to Oracle database tables so that a reconciliation can be performed to ensure that only authorized changes have been made.

- Critical audits have not been enabled in the Oracle.

The review of DCLB platform versions showed the following Operating Systems (OS) are at end of life and no longer supported by the vendor.

Server	**Purpose**	**OS**
DCLBADDC1	Primary Domain Controller	Windows 2003 Standard Ed.(32-bit)
DCLBADDC2	Backup Domain Controller	Windows 2003 Standard Ed.(32-bit)
DCLBFILE01	Home Directory, SQL	Windows 2003 Standard Ed.(32-bit)
DCLBPROD01	DC Lottery Application server	Windows 2003 Standard Ed.(32-bit)
DCLBPROD01	Application Server	Windows 2003 Standard Ed.(32-bit)

Domain Controller:

Audit Policy:

Critical audits in the system (i.e. directory service access, policy change, privilege use, and process tracking) are not currently enabled.

Password Policy:

- Complexity requirement is not turned on. Enabling this configuration will prevent unauthorized access as a result of easy to guess passwords.

Security patches are not currently applied to the server supporting the ICS application, this application is used to reconcile DC Lottery activity.

Without the appropriate Information Technology processes and procedures in place, there is increased exposure to unauthorized activity which could cause technology resources to be unavailable, thereby resulting in disruptions to government operations.

Recommendation:

We recommend that DCLB re-evaluate the stated accounts, disable those that are no longer needed, and continue the efforts of implementing procedures for entitlement review to verify that the individuals with system permissions are appropriate. We also recommend that DCLB document a secure build configuration for the OS and database supporting the ICS application. DCLB should perform periodic (e.g. semi-annual) reviews of critical configurations for OS and database that support the ICS application to verify compliance with secure configuration requirements. We further recommend that DCLB implement procedures to account for and monitor activities of DBA type accounts to include Sys User ID, SysDBA, Sysoper and Sysasm. DCLB should define password parameters for the Oracle database supporting the ICS application. Systemic reports for Oracle database table changes should be generated and reconciled with the supporting approved change request form(s) to verify that only authorized changes have been implemented. We recommend that auditing of critical events/activities in the database be turned on. DCLB should upgrade critical platforms to vendor supported OS versions. DCLB should evaluate the Domain Controller Audit Policies and enable critical audits to capture events or activities necessary in the event of research or investigation. We recommend that DCLB enable password complexity requirement and implement a process to monitor and apply timely security patches to platforms supporting the ICS application.

Management Comments:

DCLB agrees with this recommendation and will:

- Evaluate all the ICS Application accounts and verify that the accounts are needed and verify that the accounts are configured with the appropriate permissions. From the initial evaluations, the DCLB will remove the following ICS Applications accounts:
  - Lottery – Default Lottery User
  - Viewer – Default
  - Opr - Default operator

- Evaluate the Operating Systems accounts. From the initial evaluations the DCLB will remove the following Operating System accounts:
  - Guest - Default Guest

- Evaluate the Data Center physical access cards. The DCLB will complete this review with the DCLB Security Department before January 1, 2016.

DCLB agrees with this recommendation and will work with the Internal Control System vendor, Elsym Consulting, and DCLB Security to document a secure build for the Windows OS and Oracle database supporting the ICS application. The DCLB will complete this work before

February 5, 2016. In addition, before February 5, 2016, the DCLB will draft and promulgate Standard Operating Procedures for a semi-annual review of critical configurations for the OS and database supporting ICS.

DCLB agrees with this recommendation and will work with the Internal Control System vendor, Elsym Consulting, and DCLB Security to:

- develop processes and procedures for reviewing and monitoring DBA type users,
- define password parameters for Oracle,
- develop processes and procedures for reviewing Oracle table changes,
- enable auditing of critical events and activities.

DCLB will have these procedure in-place and operational by February 22, 2016.

DCLB agrees with this recommendation and is working to upgrade these servers by December 24, 2015. The DCLBADDC1 and DCLBADDC2 servers have already been updated to Windows 2012 OS versions.

DCLB agrees with this recommendation and will implement and enable auditing as soon as the Domain Controllers are migrated off of Windows 2003. In addition, DCLB will enable password complexity on the Windows 2012 Domain Controllers

DCLB agrees with this recommendation and will implement Standard Operating Procedure to monitor and apply security patches to the ICS servers. DCLB will have this procedure in-place and operational by February 22.

6. Implement Improvements Around Network Security Supporting DC Lottery

The following concerns were identified during the review of network security for the Office of the Chief Financial Officer and DC Lottery:

- The firewall rules need to be re-evaluated and refined to allow only traffic needed to support business operations. There were rules open in the firewall that allowed excessive traffic inbound.

- Redundant IPS device is not currently in place. Consequently, if the IPS becomes inoperable there would be no software to inspect and prevent malicious software from coming into the internal network.

- Data Loss Prevention (DLP) software is not currently in place. DLP software can detect and prevent unauthorized attempts to send data outside of the DC network.

Without adequate network security support in place, there is increased risk exposure to external threats.

Recommendation:

We recommend that management perform a re-evaluation of firewall rules and refine rules where needed. We recommend that management review redundant IPS to prevent traffic not being inspected that should be installed. We recommend that DLP software should be implemented to prevent data theft.

Management Comments:

Management agrees that the firewall rules should be re-evaluated and refined in light of concerns raised on limiting traffic to support business operations. Management agrees that a back-up or fail-over IPS device needs to be installed at DCLB to ensure business continuity. Management also agrees that DLP software should be added to the OCFO domain and shall engage OCTO in a discussion on how to manage DLP on the DC network.

7. Document the Review Process for the Intralot SSAE16 Report

The Lottery obtains an annual Type 2 SSAE 16 report from Intralot, which provides the gaming service system for the Lottery. The report provides an opinion on Intralot's design and operating effectiveness of controls. The report also documents the internal control objectives, control activities, test applied by the service auditor and the results of the test. The internal controls of Intralot are significant to the processes and financial reporting of the Lottery.

The Lottery obtains a copy of the annual report but does not document its policy and review process for the report. Without documentation of the policy and review process for the report, there could be potential gaps between the controls the Lottery management expects to be in place and operating effectively and the actual results of the procedures performed. This could lead to management's improper reliance on the report.

Recommendation:

We recommend that management document its policy and review process for the report and document its review of the annual report.

Management Comments:

The Lottery will implement the recommendation.

8. Continue to Develop and Redefine the Game Security Plan

As the use of technology continues to evolve, the risk of theft or loss to the Lottery continually changes. Security risks include, but are not limited to, the drawing process, warehouse security, distribution of games, payment procedures and access to IT systems. Management's effort to continuously develop and redefine its game security plan is an important control activity needed to adequately protect the integrity and security of the Lottery.

Despite the current game security plan that management has in place, SBC did not identify ongoing effort to develop and/or redefine the game security plan in order to address emerging issues. Without continuous effort to develop and redefine the game security plan, emerging issues may not be able to be addressed on a timely basis, which could compromise the integrity, security, honesty, and fairness of the gaming system.

Recommendation:

We recommend that management periodically review the game security plan and address emerging risks, in order to mitigate the Lottery's exposure to these risks.

Management Comments:

The Lottery is constantly reviewing its operational plans, and none are as important as game security and integrity. The Lottery has a secure instant ticket delivery process and secure storage in a vault outfitted with several cameras inside and outside of the vault. Swipe card and keypad access is only granted to a warehouse staff (5) and a 2 members of the finance staff. Our draw process includes the presence of a draw specialists and independent auditors. Within the past year, the lottery amended its payment terms to collect money quicker and changed its distribution process to reduce retailer overstock. The Executive team meets weekly to discuss all lottery business. In addition, a best practice study of the lottery was published in March, 2016 which rated the lottery very high (7th out of 45) overall, measuring several topics including our security (the report can be found on the OCFO's website).

9. Document Policy and Procedures for Daily Gaming Analysis

The documentation of policies and procedures for daily gaming analysis is an important control activity that can mitigate the risk of error or fraud in the gaming system. The Lottery does not have daily gaming analysis policy and procedures documented and in place.

The lack of policies and procedures related to daily gaming analysis could result in errors or fraud in the gaming system. The implementation of daily gaming analysis allows the Lottery to identify unusual trends and serves as a way to monitor retailers and Intralot activity. Such monitoring will improve the internal controls over the gaming activities.

Recommendation:

Management should establish policies and procedures to analyze daily gaming activity for unusual trends.

Management Comments:

The executive team of the lottery gets daily emails of all daily game draws. The emails list the sales and the liability for each of the draws. In addition, for some of our games that have several draws a day, our security team receives an alert when a retail location reaches a certain sales dollar threshold. At the final alert level, the retailer's terminal is temporarily disabled and a phone call is placed to the retailer to verify the legitimacy of the sales. Once verified, the terminal is immediately enabled. In addition, a best practice study of the lottery was published in March, 2016 which rated the lottery very high (7th out of 45) overall, measuring several topics including our draws (the report can be found on the OCFO's website).

NOT-FOR-PROFIT HOSPITAL CORPORATION

10. Self Report Medicare Non-Compliance*

When the United Medical Center (the "Hospital") was foreclosed upon and taken over by the District in 2010 there were some Medical Center arrangements with referring physicians that may have failed to comply with Center for Medicare and Medicaid Services regulations. On December 1, 2015, with the assistance of outside counsel, the hospital reported the matters to the Center for Medicare and Medicaid Services under the self-referral disclosure protocol.

Additionally, the Hospital is working with the Center for Medicare and Medicaid Services (CMS) on the repayment of the Primary Care physicians' billings overpayments identified as a result of the Hospitals's voluntary self-audit of Medicare Part B nonfacility-coded point of service physician claims during 2010 through 2012. The Hospital identified nonfacility-coded physician claims that were billed by the Hospital as well as the physician providing the service.

In December, 2015, the Hospital notified the Center for Medicare and Medicaid Services of potential billing errors related to billing of acute psychiatric Medicare services. The Hospital billed some psychiatric Medicare patients under the distinct part NPI number which is reimbursed at a different per diem rate.

Without proper oversight over the compliance with CMS rules, regulations and laws, there is the potential of other violations not being identified which exposes the Hospital to further liability.

The estimated liabilities recorded by the Hospital for the self-referral disclosure, Primary Care Physician billings, and Psychiatric billing was approximately $1,533,000.

Recommendation:

We recommend that the Hospital continue to actively pursue the resolution of these existing violations and establish regulatory reporting policies around internal compliance. The Hospital should establish timely communication and resolution relative to compliance issues.

Management Comments:

Management concurs with the finding and recommendation. Over the last several years, the Hospital recognized that there may be exposure as it relates to compliance with contracts and agreements. The Hospital took the necessary steps to identify the various issues. The Hospital engaged an outside firm to assist with this process. Upon completion of that project in August 2015, the Hospital then notified the appropriate parties. The process for completing this review has not been completed. We will continue to work with the appropriate authorities.

We have also instituted a process of having our agreements reviewed by our Chief Financial Officer and General Counsel. We are in the process of recruiting a Chief Compliance Officer to enhance our program.

*Reported as a material weakness in the Not-for-Hospital's financial statements.

11. Create a Formal Review Process for Changes to Employee Records and Updating Employee Deductions**

The Hospital has a Position Review Committee (PRC) made up of the Medical Center's executive team that has the authority to approve or disapprove all requests to fill vacant positions, requests for additional staffing as well as transfer of full-time equivalents (FTEs) to other cost centers. For 9 of the 12 months of the fiscal year ended September 30, 2015, some samples selected for testing did not include evidence to support that the new positions were approved. Management noted that they had remediated the issue for the last three months of the fiscal year; however, the HR policy was not updated with the new PRC process as well as HR process of tracking the positions.

We noted based on review of the HR File policy that there are minimum data sets that were required to be in each employee's personnel file. A New Hire Checklist is used to review the file content to ensure compliance with DOH requirements. We noted that the review of the New Hire Checklist was not being timely performed and in some cases up to 11 months which was evidenced by some checklists being partially completed or some missing in the file.

We further noted that new hire details as well as updates of other employee information entered into the Hospital's Meditech system were not reviewed to ensure completeness and accuracy of the employee's personnel data. We noted instances where some employees were not being paid using the correct pay rates. We further noted that the human resources (HR) department did not

have a formal process for ensuring the completeness and accuracy of the deductions made from employees pay related to various benefits which include health insurance, life insurance, etc. We noted instances where the deduction was more, less or none based on the required deduction. In other instances, a request to stop the deduction was made; however, deductions continued. During the nine months ended September 30, 2015, the Hospitals paid an additional $454,395 due to lack of proper controls within the HR department to ensure the appropriate amounts were being deducted and that the third party providers were being updated on any changes to add or remove employees or their beneficiaries within a reasonable time period.

According to the District of Columbia Municipal Regulations for Hospitals section 2016.2, "Each hospital shall ensure and maintain evidence of, for employees and contract staff, current active licensure, registration, certification or other credentials in accordance with applicable District of Columbia law, prior to staff assuming job responsibilities and shall have procedures for verifying that the current status is maintained".

Lack of a formal process of reviewing personnel data entered into the Meditech system to ensure the completeness and accuracy of the data.

Lack of timely second level review to ensure that all required paperwork is included in the employee files and are being properly documented.

Lack of proper controls to ensure that all deductions are being properly made and the third party providers are notified of any changes within a reasonable time period.

Without proper review and approval of personnel data including pay rates entered into the Meditech system, the data could be improperly recorded and go undetected. Additionally, employees may be hired that do not meet the Medical Center's standards as well those set by the Department of Health and expose the Medical Center to potential liability.

The lack of adequate controls over the deduction process has led the Medical Center to pay for more than its share of the cost.

Recommendation:

We recommend that management document their review of employee records for proper approval of position, pay rate, union status, and DOH compliance among other important attributes.

We also recommend that the HR department develop procedures and controls to ensure that appropriate updates to employees' deductions as well as notifications to the third party providers are done on a timely basis.

Additionally we recommend the update of the PRC policy as well as other HR policies as appropriate. Policy change and communication protocols should be established to ensure they are timely communicated to employees and management.

Management Comments:

Management concurs with the finding and recommendation. Management will review regularly the PRC policies and procedures and update as appropriate. HR Management will review on regular basis content within the employee personnel files that may require compliance with DOH and other regulatory agencies. Management has directed the Human Resources department (HR) to work with Information Technology (IT) to develop reports allowing a secondary review by HR Management of data elements entered into Meditech for each employee and document such review. Full implementation is expected by June 30, 2016.

Management has directed the HR department to work in conjunction with the third party vendors to ensure accuracy of employee deductions. In addition, HR will begin training managers to provide timely information on employee activity to increase HR efficiency and timeliness. Also, Finance will work in conjunction with HR to ensure accuracy of monthly vendor statements and subsequent payments. These actions should be effective by June 30, 2016.

** Reported as a significant deficiency in the Not-for-Profit stand alone financial statements.

12. Improve Controls Over Financial Statement Close Process**

We noted during our review of the financial statement close process that there were no written procedures. Additionally there were no formalized account level reconciliation documentation and review by management and as a result we noted instances of incorrect reconciliations of accounts.

Specifically, we noted there was not a detail review of reconciling items on the bank reconciliations and in one instance an amount was recorded as a deposit in transit for several months even though the cash had already been deposited and processed by the bank. Additionally, we reviewed different bank reconciliations and noted there was not a review to ensure that all wire transfers were posted as part of the bank reconciliation and there were three transfers on the bank statement that were not recorded in the general ledger yet the bank reconciliation was completed.

There were also instances in which the information provided to the Hospital's reimbursement consultant to complete the contractual allowances, bad debt and credit balance review were not correct as well as the requested adjustments were not properly recorded in the general ledger.

Lack of adequate review could lead to the financial statements not being fairly stated and errors not being addressed on a timely basis.

Recommendation:

We recommend that the Hospital draft written procedures regarding the financial close process which includes support of the completed reconciliation, review and approval by a secondary reviewer.

We also recommend that a detail review be performed with sufficient documentation regarding reconciling items for monthly cash reconciliation as well as all reconciled accounts. In addition, a review should be performed on the data provided to the consultant to ensure that it is accurate as well as making sure that the general ledger accounts agree to the amounts given to the consultant.

Management Comments:

Management concurs with the finding and recommendation. Hospital management will include the current journal entry checklist and closing schedule into a formal policy, including procedures, for the monthly and year-end close process. Management will use current OCFO policies when applicable. Management will adopt a formal policy which will include all balance sheet account reconciliations and review processes on a monthly basis, ensuring the reconciliations are accurate, timely and reviewed by Finance senior management. Management will adopt a policy, with procedures, to ensure accurate calculation of contractual allowances against accounts receivable and review these calculations on a monthly basis with the reimbursement specialist or consultant. These updated policies and procedures will be in place by June 30, 2016.

** Reported as a significant deficiency in the Not-for-Profit stand alone financial statements.

13. Create a Formal Process of Adjusting Patient Revenue Charges for the Skilled Nursing Facility (SNF)

Changes to the SNF room rates require the authorization by the Hospital management

SNF residents are required to complete and sign an admission packet which contains a contract that includes among other items the charges for services provided to residents that pay out-of-pocket for their stay. The admission contract is signed by the resident and the Hospital and SNF representative. The new resident contract revised on January 1, 2015, had a private pay rate of $500. We noted however residents were being billed at $450 for the period after January 1, 2015.

Management noted that any change in room rates require the authorization of the CFO. In this case an increase in private pay rate was not authorized by the CFO nor was it communicated to Patient Financial Services. As such, the SNF was communicating information to residents which was not in line with what was charged or authorized.

Lack of a formalized process may lead to improper revenue recognition and loss of revenue.

Recommendation:

We recommend that the Hospital create formal written policies and procedures for the SNF operations that would include the patient charges change policy and patient communication and contract review by Hospital management to ensure what is communicated to patients is in line with Hospital policy.

Management Comments:

Management will develop a formal policy that will address the pricing for patient rooms in the Skilled Nursing Facility (SNF). This policy will include making the patient (resident) aware of the current room rate in effect at the time of admission. The policy will address changes to the room rate and securing and documenting proper authorization from the CFO or CEO prior to the room rate being charged to the resident bill. The policy will also address the personnel authorized to make changes to the room rate, with proper authorization. The policy will be developed and reviewed by the patient financial services (PFS) department, as well as management within the SNF department. This policy will be written, reviewed and in effect by June 30, 2016.

14. Implement Monitoring Procedures for the Point Click Care System for the Skilled Nursing Facility (SNF)

Complementary user entity controls are those controls for which the service organization recommends to be in place at user entities in relation to the services performed by the service organization to help ensure that the controls at the service organization are operating at optimum. These complementary user entity controls are a critical component of any statement on standards for attestation engagements (SSAE) 16 assessment, as it illustrates to the intended user of the report that the user entity has certain roles, responsibilities, and obligations in helping the service organization achieve the control objectives stated in the description of the "system".

Point Click Care is the system used by the SNF for billing and financial reporting. Management does not review the Point Click Care (PCC) System Statement on Standard for Attestation Engagement (SSAE) No. 16 (SSAE 16) Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting. As such management does not also review and verify that the appropriate Complementary User Entity Controls are in place.
We noted an instance where a claim was billed at the wrong amount instead of the flat Medicaid rate and as such manual intervention was required to send a new claim.

Management is responsible for ensuring that they safeguard the assets of the Hospital and lack of review of the SSAE 16 report and the complementary user entity controls may cause there to be inadequate internal controls over financial reporting to prevent errors or fraud.

Recommendation:

We recommend that management obtain and review the SSAE 16 report for PCC at least annually and review it for any exceptions that are reported and determine if those exceptions have any adverse effect on the Hospital and develop corrective action if needed. Additionally, we recommend the SNF review the PCC recommended complementary user entity controls and ensure that they are implemented and are operating effectively so as to ensure that the controls at the service organization are functioning as they should.

Management Comments:

Management concurs with the finding and recommendation. Management has since obtained a copy of the required SSAE 16 for the PCC system. Management will review the user entity controls and ensure end users are complying with them. The Medical Center Controller will oversee and review the complementary user entity internal controls on a quarterly basis, beginning June 30, 2016, and note any deficiencies within the report. If the user controls are not functioning as required, the end users should document the deficiency and report back to the Controller, who in turn should report back to PCC.

15. Develop a Process to Ensure Completeness of Application of the Appropriate Contractual Adjustment Against Accounts Receivables

Proper review and approval by management should be performed to ensure the accounts receivable reported are fairly stated.

We noted an instance in which a patient account did not have any contractual adjustment taken after cash was remitted by the third party payer. In another instance there were two related patient accounts; one being the primary account (mother) and the other as the secondary account (baby) that were not both appropriately updated for payment remitted to the hospital. Payment for both accounts was inappropriately recorded in only the primary account and therefore the secondary account was still showing an outstanding balance.

The lack of second level review of all accounts for which payment has been received may lead to amounts being inappropriately and inaccurately reported as due from patients.

Recommendation:

We recommend that a second level review be performed and management utilizes some of the available reports within the Meditech system to increase efficiencies. Additionally management should ensure that the associated staffs are properly trained.

Management Comments:

Management will request Information Technology (IT) to explore the capability of merging the patient accounts of mother and baby(s) within Meditech where applicable. The patient financial services (PFS) department senior management will conduct a periodic review of accounts to ensure that the existing process of baby accounts are combined with the mother's account and that both accounts are reviewed concurrently for proper posting of cash payments and contractual adjustments. This procedure should be effective by June 30, 2016.

Management will ensure that a review and appropriate action of accounts with credit balances will be conducted on a regular basis, according to the guidelines stated in PFS policy 300. Management will ensure that the Director of Patient Financial Services (or designee) will perform a secondary review of adjustments made to the credit balance accounts and accounts with outstanding balances after payments and contractuals have been posted, and to ensure that proper procedures are followed as prescribed in this policy. Management will ensure that the Patient Financial Service (PFS) staff will be properly trained by reviewing a log maintained by PFS management of training meetings and documenting the purpose and attendees. This should be effective by June 30, 2016.

16. Review And Reconcile Changes To Charge Master

The criteria for identifying and testing the general information technology controls can be mapped to the National Institute of Standards and Technology (NIST).
The Federal Information Security Act (FISMA) of 2002 was put in place to implement a framework for the effectiveness of information security controls for Federal information systems. FIMSA gave NIST the authority to develop guidelines for implementing and maintaining information security programs. NIST Publication 800-53 revision 4: Security and Privacy Controls for Federal Information Systems and Organizations was considered in performing our review.

Currently a report is not being generated and reconciled to authorized change tickets to ensure that only authorized changes have been made.

The charge master is critical to ensuring the accuracy of fees billed patients for services rendered.

Recommendation:

A report should be sent to the Charge Master Team whenever changes are made to the Charge Master. The changes on the report should be reconciled to the supporting authorization to verify that all changes made to the The Medical Center Charge Master were authorized.

Management Comments:

Management concurs with the finding and recommendations.

After making a comprehensive assessment of the CDM process, the Information Technology department will create a monthly report from the MIS dictionary, i.e., print dictionary audit trail. This report will be automatically sent to the Finance Department to review and audit the changes made to the charge master. Any discrepancies noted will be addressed by the charge master team and corrections will be made accordingly. The charge master team will also revise the policy and procedure to reflect the new audit reporting process.

17. Develop An Assessment And Plan For Information Technology (IT) General Controls

The criteria for identifying and testing the General Information Technology Controls can be mapped to the National Institute of Standards and Technology (NIST).

The Federal Information Security Act (FISMA) of 2002 was put in place to implement a framework for the effectiveness of information security controls for Federal information systems. FIMSA gave NIST the authority to develop guidelines for implementing and maintaining information security programs. NIST Publication 800-53 revision 4: Security and Privacy Controls for Federal Information Systems and Organizations was considered in performing our review.

The review of Information Technology support processes at the Medical Center identified the following concerns:

- Third party governance and oversight: The Medical Center relies on a 3rd party (Park Place) for data center support for the hardware and network communications to the critical application Meditech. However currently a process (e.g., SSAE 16 or similar type assessment) is not in place to ensure that Park Place maintains the expected Information Security and related technology controls over The Medical Center data and technology resources.
- Network Segmentation: The review of the Hospital's network architecture indicates that critical servers supporting the local area network reside in the default VLAN1. Security guidance recommends that critical technology resources not reside in the default VLAN1 because this VLAN is known to the external communities that may try to gain unauthorized access to The Hospital. The network segmentation has no direct effect on the Meditech application given that it is hosted at the 3rd party premise.

- *Firewall rules*: The review of the Hospital's firewall rules indicates that rules have not been consistently refined to open on the ports/services that are needed to support the Medical Center business operations. SBC reviewed the firewall rules and observed rules defined as "Any". Defining firewall rules as "Any" increases the exposure and risk to unauthorized traffic on the Hospital internal network.
- *Network Scanning*: Currently a process is not in place to perform periodic scanning of the Medical Center network. As a result, potential vulnerabilities may not be identified and remediated timely.

As a result, there is increased risk exposure to unauthorized access attempts which could lead to theft of data or short term disruption of operations.

Recommendation:

The Hospital should implement a periodic assessment to ensure that Park Place is maintaining the expected level of information security and related controls over technology resources. The Medical Center should develop a plan to transition critical servers out of the default VLAN1. The Hospital should implement a review to strategically refine over time the firewall rules to only open the ports/services required to support the business operation. The Medical Center should pursue performing quarterly or annual scanning of the network in order to timely identify and remediate potential vulnerabilities.

Management Comments:

Management concurs with the findings and recommendations.

Park Place currently provides the Medical Center up-to-date SSAE16 certifications along with the detailed reporting of the controls audited. Management is in the process of updating its security policies to include continual auditing of security controls in place at their 3rd party vendors. Management is currently executing a project to revamp its infrastructure. This initiative includes migrating all systems to their appropriate VLAN. All critical systems will be moved off VLAN1 to their appropriate VLAN. Further, management is currently executing an infrastructure modernization project to revamp all aspects of the Medical Center's environment. This initiative includes reviewing all firewall rules for accuracy and with the intent to restrict only necessary traffic allowed in/out of our network. As part of management's security plan, management is enlisting a 3rd party vendor to perform bi-annual penetration and vulnerability testing against the Medical Center's data center and Park Place. The test was completed on December 7, 2015 and final report was received December 22, 2015 by Pendulum.