DISTRICT OF COLUMBIA
OFFICE OF THE INSPECTOR GENERAL

OIG Project No. 19-1-20MA

February 2019

GOVERNMENT OF THE DISTRICT OF COLUMBIA

MANAGEMENT RECOMMENDATIONS FOR FISCAL YEAR 2018

Guiding Principles

*Workforce Engagement * Stakeholders Engagement * Process-oriented * Innovation * Accountability * Professionalism * Objectivity and Independence * Communication * Collaboration * Diversity * Measurement * Continuous Improvement*

Mission

Our mission 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 programs and operations; and

- recommend and track the implementation of corrective actions.

Vision

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

Core Values

Excellence * Integrity * Respect * Creativity * Ownership
* Transparency * Empowerment * Courage * Passion
* Leadership

WE ARE
WASHINGTON
DC

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Inspector General

Inspector General

OIG

February 6, 2019

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 Chief Financial Officer DeWitt:

Enclosed is the District of Columbia Management Recommendations report SB & Company, LLC (SB&C) issued for fiscal year (FY) 2018 (OIG No. 19-1-20MA). SB&C submitted this report as part of our overall contract for the audit of the District of Columbia's general-purpose financial statements for FY 2018.

This report sets forth SB&C's comments and recommendations intended to improve internal controls or result in other operating efficiencies in District government. The report also includes SB&C's summary of prior years (FYs 2017 & 2016) management recommendations and the corresponding implementation status.

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

Sincerely,

Daniel W. Lucas
Inspector General

DWL/ws

Enclosure

cc: See Distribution List

DISTRIBUTION:

Mr. Rashad M. Young, City Administrator, District of Columbia (via email)
Mr. Barry Kreiswirth, General Counsel, City Administrator, District of Columbia (via email)
The Honorable Charles Allen, Chairperson, Committee on the Judiciary and Public Safety, Council of the District of Columbia (via email)
The Honorable Anita Bonds, Chairperson, Committee on Housing and Neighborhood Development, Council of the District of Columbia (via email)
The Honorable Mary M. Cheh, Chairperson, Committee on Transportation and the Environment, Council of the 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 Vincent C. Gray, Chairperson, Committee on Health, Council of the District of Columbia (via email)
The Honorable David Grosso, Chairperson, Committee on Education, Council of the District of Columbia (via email)
The Honorable Kenyan R. McDuffie, Chairperson, Committee on Business and Economic Development, Council of the District of Columbia (via email)
The Honorable Brianne K. Nadeau, Chairperson, Committee on Human Services, Council of the District of Columbia (via email)
The Honorable Elissa Silverman, Chairperson, Committee on Labor and Workforce Development, Council of the District of Columbia (via email)
The Honorable Brandon T. Todd, Chairperson, Committee on Government Operations, Council of the District of Columbia (via email)
The Honorable Robert C. White, Jr., Chairperson, Committee on Facilities and Procurement, Council of the District of Columbia (via email)
The Honorable Trayon White, Sr., Chairperson Committee on Recreation and Youth Affairs, Council of the District of Columbia (via email)
Mr. John Falcicchio, Chief of Staff, Executive Office of the Mayor (via email)
Ms. LaToya Foster, Interim Director of Communications, Office of Communications, Executive Office of the Mayor (via email)
Ms. Jennifer Reed, Director, Office of Budget and Performance Management, Office of the City Administrator (via email)
Ms. Nyasha Smith, Secretary to the Council (via email)
The Honorable Karl Racine, Attorney General for the District of Columbia (via email)
Mr. Timothy Barry, Executive Director, Office of Integrity and Oversight, Office of the Chief Financial Officer (via email)
The Honorable Kathy Patterson, D.C. Auditor, Office of the D.C. Auditor, Attention: Cathy Patten (via email)
Mr. Jed Ross, Director and Chief Risk Officer, Office of Risk Management (via email)
Ms. Berri Davis, Director, FMA, GAO, (via email)
Mr. Graylin (Gray) Smith, Partner, SB & Company, LLC (via email)

Government of the District of Columbia

Management Recommendations

For the Year Ended September 30, 2018

SBC

SB & COMPANY, LLC
KNOWLEDGE • QUALITY • CLIENT SERVICE

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

In planning and performing our audit of the basic financial statements of the Government of the District of Columbia and related entities (the District) as of and for the year ended September 30, 2018, 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 controls over financial reporting (internal controls) as a basis for designing audit procedures that were appropriate in the circumstances 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 District's internal controls. Accordingly, we did not express an opinion on the effectiveness of the District's internal controls over financial reporting.

Our consideration of internal controls was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal controls that might be significant deficiencies or material weaknesses, and therefore, there can be no assurance that all deficiencies, significant deficiencies, or material weaknesses have 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 controls 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 controls, 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 controls were considered to be a material weakness.

This letter does not affect our report dated January 23, 2019, 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 controls or result in other operating improvements.

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.

SB + Company, LLC

Washington, DC
January 23, 2019

TABLE OF CONTENTS

GENERAL GOVERNMENT

GENERAL GOVERNMENT

1. Update unsupported SQL Server software Supporting iNovah

iNovah is a point-of-sales system used by District agencies to allow citizens and businesses to procure goods and services. The application is configured to allow each agency to record their transactions using location-specific tender types; all agencies will allow customers to use checks or payment cards but only some agencies are allowed to receive cash. The application has a centralized database to which all transaction activity is updated daily, and the database is also the source for updates to the general ledger.

The version of server software used to support the iNovah application is at end of life and is no longer supported by the vendor. As a result, should a concern be identified in the operation of the software, with the version being out of the production cycle, the software flaw may not be addressed timely.

Recommendation

SB & Company, LLC (SBC) recommends Office of the Chief Financial Officer (OCFO) to continue the efforts of migrating to a more current version of the SQL Server.

Management Response

The existing Windows 2008 R2 iNovah production servers are scheduled to be retired as soon as testing of the Windows 2016 servers with a new release of iNovah supporting EMV chip technology is completed and the new production servers can be migrated to production.

2. Use Encryption to Secure Data

Processes are not in place to encrypt the back-up tapes which maintain data for the OCFO. Therefore, if the tapes were compromised or stolen, there is exposure to unauthorized access to the data.

Recommendation

SBC recommends OCFO to continue the efforts of data classification and implement encryption of critical data in back up tapes to protect the data per the data classification policy.

Management Response

Management concurs that the backup tapes should be encrypted and shall direct the team to test and implement encryption as soon as possible. The overall approach to data classification by the District as a whole, and within the OCFO in particular, will result in a better understanding as to the sensitivity of the data and the rules to protect the data, based upon the classifications established, should be applied to all backups as appropriate.

3. Implement a Risk Management Framework to Comply with National Institute of Standards and Technology (NIST) Publication 800-37

NIST Publication 800-37 defines the objectives for having a Risk Management Framework for Information Systems. The objectives per NIST 800-37 to be accomplished through a Risk Management framework for Information Systems include providing a repeatable process designed to promote the protection of information and information systems commensurate with risk; and placing emphasis organization-wide on the preparation necessary to manage security and privacy risks. The Office of Chief Technology Officer (OCTO) has not documented a Risk Management framework that complies with NIST 800-37.

Recommendation

SBC recommends OCTO implements a Risk Management framework that complies with NIST 800-37.

Management Response

OCTO acknowledges the finding and is in process of staffing the Governance, Risk, and Compliance (GRC) division that will be responsible for implementation of Information Technology Risk Management framework that complies with NIST 800-37.

As part of the plan OCTO is hiring a GRC Manager to lead the effort. The GRC manager will be responsible for the overall functions of the group and will lead the development and implementation of the Risk Management Framework. The GRC team will review existing policies and will revise and update policies where applicable including the identified OCTO policy 1050.2.

As part of the work started in 2017, OCTO completed the rollout of a GRC management platform that will compile a complete picture of technology and security-related risks and understand their impact to improve decision-making. This platform also serves as a flexible environment to manage district-wide IT policies and ensure alignment with compliance obligations with ability to assign ownership of IT and security controls and map policies and controls to key business areas and objectives.

4. Patch Updates to Peoplesoft and Supporting Infrastructure (Operating System and Database)

Operating system and database patches are not always installed timely. Delays in applying patches can increase risk to vulnerabilities that could successfully disrupt the availability of critical applications to process transactions.

Recommendation

SBC recommends that the patch updates be applied to PeopleSoft and supporting infrastructure.

SBC recommends OCTO Management more formalize the flaw remediation process to require certain approvals, for example risk acceptances, to be approved if patch updates cannot be applied timely.

SBC also recommends that the process include specific timeframes and monitoring be put in place on the timeliness of applying patch updates.

Management Response

When OCTO's Citywide IT Security (CWITS) group has identified risks or critical patches in the application or database, a security waiver process is in place where the program must seek approval from OCTO Executive Management by completing and submitting a security waiver form, if they wish to defer the implementation of the patches/updates for longer than a 3 to 6-month timeframe.

A routine scan of the PeopleSoft infrastructure was completed by CWITS on Friday, April 27, 2018. The Application Team engaged the Enterprise Cloud and Infrastructure Services (ECIS) Team to coordinate with the vendor, Oracle Corp., to schedule the patch maintenance service request. Maintenance on the hardware is performed by the vendor, as the hardware (Oracle's Engineered Systems: Exadata & Exalogic) are self-contained appliances monitored and maintained by the vendor. The first date provided by the vendor was June 16, which was within the 3 to 6-month patching timeframe.

The vendor proposed three available dates/timeframe where they could implement the patches. OCTO scheduled the first maintenance for June 16th, and the vendor confirmed the service request. During the week of the scheduled maintenance, OCTO Executive Management chose to defer the patching because a critical initiative, to calculate and implement the Cost of Living Wage Adjustments for three years, retroactively, was occurring during the week of deployment and the program could cut into the weekend, potentially impacting the patching activities.

Due to the deferral, ECIS coordinated with the vendor once more to secure two more dates. ECIS confirmed with Oracle that the patching activities would now be scheduled for July 29. The second date was then deferred due to the implementation of the Public-Sector Workers Compensation Program, where the deployment date was advanced due to project constraints.

Because the deferrals were initiated at the Executive-level and not at the Program-level, a request for waiver from the Program was not completed. The vendor's third available option, October 7th, was confirmed and exercised, where the Exalogic servers were successfully patched by the vendor.

5. Use PeopleSoft to calculate certain Earnings Codes

Certain earnings codes which are handled manually or outside of the PeopleSoft application should be re-evaluated to determine if the earning code calculation can be automated in Peoplesoft.

Recommendation

SBC recommends PeopleSoft application programmers follow-up to determine the calculations and if the amounts paid to employees under these earning codes can systemically be completed by the PeopleSoft application.

Follow-up should be performed with agencies where it makes sense to automate in the PeopleSoft application the calculation of employee pay for these earnings codes.

Management Response

OCTO commenced collaboration with the Office of Pay and Retirement Services (OPRS) to research and determine if the Retro Pay system can be fully implemented and transitioned from OCTO to OPRS. The Retro Pay System is used to calculate mass payments in PeopleSoft.

Currently, OCTO manually runs Retro Pay program and the results are validated by corresponding agencies and OPRS. Once validated, the confirmed calculated payment amounts are loaded into the Production system. Transitioning to OPRS will allow the system to automatically calculate retro-payment amounts.

OCTO will also work with OPRS to research the feasibility of automating the process and calculations of additional compensation, administrative allowances and language fluency payments in a cost effective manner.

Longevity payment amounts for MPD are currently calculated by the system and is based on an individual employee's years of service as determined by the value entered into the service computation date field.

Finally, adjustment earnings codes are used when check reversals-adjustments are processed. When an employee is overpaid, and the check or overpayment cannot be retrieved, this process is used to recalculate the original check and reverse the errant check. Automation of the adjustments is not feasible.

6. Improve the Segregation of Duties – Change Management [Department of Employment Services (DOES)]

A procedure is not in place to ensure that the individual who makes the program change is not the same person who is requesting the super user identification to implement the change to the production environment. Therefore, duties related to making the changes and implementing the change may not always be handled by different individuals to allow for adequate segregation of these responsibilities.

Recommendation

SBC recommends that the current process used to approve the use of the super user ID to implement District Online Compensation System (DOCS) and District of Columbia Unemployment Tac Accounting System (DUTAS) changes to production be expanded so that the Information Security Officer (ISO) verifies that the individual requesting the ID to implement the change is not the same individual that made the change. When business reasons require the changes to be made and implemented by the same individual, the ISO should document the reason for approving the exception.

Management Response

The risk to the condition stated above, as it relates to segregation of duties, impacts DUTAS environment only. DOCS development team utilizes a process, in place, which assures and documents segregation of duties, as it relates to DOCS production changes. Based on this premise, the agency concurs with the need to:

- Establish a process, within the DUTAS development workflow, that affords segregation of duties between User Acceptance Testing (UAT) and production moves.

- Improve upon the Super ID request and approval process, to include validation inclusion, for both DOCS and DUTAS, whenever such request pertains to production moves (i.e. moving UAT changes to production).

It should be noted that 99% of all DUTAS changes, that required a Super ID request, between Oct 2017 and July 2018, were not related to moving changes to production and hence, would not have required a segregation of duties validation. The overall risk to this condition was therefore minimal, when viewed within the aforementioned context.

7. Improve the Controls Over the Out-Lease Monthly Cash Receipts

The Department of General Services (DGS) has three types of revenue streams: out-lease (long-term leases), short-term leases, and eastern market vendor stall/event rental. Out-lease cash receipts are tracked manually in an Excel sheet by DGS Accounting. SBC noted a reconciliation process of cash receipts of out-leases maintained by DGS Accounting against the lease agreements kept by the DGS Portfolio Management Group is not occurring.

Recommendation

SBC recommends management to consider developing an automated tracking system for out-lease agreements cash receipts due from tenants and formalize a reconciliation process between DGS Accounting and DGS Portfolio Management Group. This will ensure the revenue processing is done in accordance with policies and procedures as per D.C. Code § 10-551.02(3)(D).

Management Response

Management concurs with the auditor's finding related to Agency AM0, Department of General Services (DGS). Since January 2018, the Portfolio Management Division has worked with a third party vendor to reconcile DGS's Outlease portfolio and develop the necessary protocols to begin actively administering the Outlease portfolio within ARCHIBUS, the agency's Integrated Workplace Management System. To this end, we have abstracted all active and expired lease/license agreements that comprise the Outlease portfolio and have completed payment reconciliations for the majority of those agreements. We expect the reconciliation process will be completed over the course of the coming months. Additionally, in January 2019, we plan to "go-live" and begin invoicing and reconciling tenant accounts on a monthly basis within ARCHIBUS. We are confident that these steps will solve for the issues identified in the audit.

STATUS OF PRIOR YEAR MANAGEMENT RECOMMENDATIONS

Listed below is the status of our previous recommendations that had either been resolved or partially resolved or not resolved as of September 30, 2018.

MANAGEMENT RECOMMENDATIONS – FY17		
	RECOMMENDATIONS	STATUS
GENERAL GOVERNMENT		
1	Establish Oversight Process for Third- Party Service Providers	Resolved
2	Encrypt iNovah Data	Not Resolved
3	Refine Firewall Rules to Allow Ports and Services Needed to Support Business Operations	Resolved
4	Obtain OFOS Approval for Direct Voucher Payments	Resolved
5	Maintain Files Supporting Medicaid Eligibility	Partially Resolved
OFFICE OF LOTTERY AND CHARITABLE GAMES		
6	Implement Periodic Review of Systems Permissions	Resolved
7	Develop Vulnerability Scan Procedures for Timely Remediation of Critical Risks	Partially Resolved
UNITED MEDICAL CENTER		
8	Use Appropriate Encryption Levels to Protect Data in Storage at the Cloud Service Provider	Resolved
9	Enhance Controls over Domain Administrator Accounts	Resolved
GOVERNMENT OF THE DISTRICT OF COLUMBIA OTHER POST-EMPLOYMENT BENEFITS FUND		
10	Review and Approve Third-Party Adjustments and Journal Entries	Resolved
UNIVERSITY OF THE DISTRICT OF COLUMBIA		
11	Enhance Controls over Technology Support Processes	Partially Resolved

MANAGEMENT RECOMMENDATIONS - FY16		
	RECOMMENDATIONS	STATUS
GENERAL GOVERNMENT		
1	Processes Are Not in Place to Ensure Data is Secured Based on the OCTO Data Classification Policy	Partially Resolved
2	Medicaid Eligibility Files Were Not Provided to Auditors	Partially Resolved