Audit Report

Department of Budget and Management
Office of Personnel Services and Benefits

May 2019

OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

For further information concerning this report contact:

Department of Legislative Services
Office of Legislative Audits
301 West Preston Street, Room 1202
Baltimore, Maryland 21201
Phone: 410-946-5900 · 301-970-5900
Toll Free in Maryland: 1-877-486-9964
Maryland Relay: 711
TTY: 410-946-5401 · 301-970-5401
E-mail: OLAWebmaster@ola.state.md.us
Website: www.ola.state.md.us

The Office of Legislative Audits operates a Fraud Hotline to report fraud, waste, or abuse involving State of Maryland government resources. Reports of fraud, waste, or abuse may be communicated anonymously by a toll-free call to 1-877-FRAUD-11, by mail to the Fraud Hotline, c/o Office of Legislative Audits, or through the Office's website.

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Victoria L. Gruber
Executive Director

Gregory A. Hook, CPA
Legislative Auditor

May 14, 2019

Senator Craig J. Zucker, Co-Chair, Joint Audit Committee
Delegate Shelly L. Hettleman, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have conducted a fiscal compliance audit of the Department of Budget and Management (DBM) – Office of Personnel Services and Benefits (OPSB) for the period beginning April 16, 2014 and ending September 7, 2017. OPSB develops the State's personnel policies, administers the health care benefits programs for State employees and retirees, and has other responsibilities, including salary administration and classification, recruitment and examination, and employee relations. OPSB also provides centralized support to agencies for the State's Statewide Personnel System (SPS).

Our audit disclosed that OPSB had not provided guidance to agencies using SPS to assist them in establishing adequate controls over the processing of payroll adjustments nor developed internal procedures for ensuring that only valid and authorized payroll adjustments were processed in SPS. Adjustments resulting in State employee pay increases of approximately $5.7 million were processed in SPS in calendar year 2017. In addition, certain critical transactions processed in the OPSB-maintained employee health care benefits administration system (BAS) were not subject to adequate review and approval, and OPSB employee access to the system was not periodically reviewed to ensure that access was properly restricted. We noted a number of employees with unnecessary critical access in the system.

Our audit also disclosed a lack of sufficient controls to ensure that all collections were deposited. Collections primarily included prescription drug rebates and certain health insurance premium payments and totaled approximately $147.1 million during our audit period. Furthermore, individual files maintained on BAS containing sensitive personally identifiable information (PII) pertaining to various

health insurance vendors were being stored in clear text without adequate safeguards. OPSB also lacked assurance that all necessary information technology security and operational controls existed over its flexible spending account system, which was hosted, operated, and maintained by a third-party service provider under contract with OPSB.

Finally, our audit included a review to determine the status of five findings contained in our preceding audit report. We determined that OPSB satisfactorily addressed four of these findings, with the remaining finding repeated in this report.

DBM's response to our findings and recommendations, on behalf of OPSB, is included as an appendix to this report. We reviewed the response and noted general agreement to our findings and related recommendations, and we will advise the Joint Audit Committee of any outstanding issues we cannot resolve with OPSB.

We wish to acknowledge the cooperation extended to us during the audit by OPSB. We also wish to acknowledge DBM's and OPSB's willingness to address the audit issues and implement appropriate corrective actions.

Respectfully submitted,

Gregory A. Hook

Gregory A. Hook, CPA
Legislative Auditor

Table of Contents

* **Denotes item repeated in full or part from preceding audit report**

Background Information

Agency Responsibilities

The Department of Budget and Management (DBM) – Office of Personnel Services and Benefits (OPSB) directs the development of personnel policies for State agencies in the Executive Branch under the State Personnel Management System.[1] OPSB also administers the health care benefits programs for State employees and retirees, and the flexible spending accounts for State employees. OPSB has a variety of other responsibilities, including salary administration and classification, recruitment and examination, and employee relations, and provides centralized support to agencies for the State's Statewide Personnel System.

Statewide Personnel System

OPSB's Statewide Personnel System (SPS) provides a comprehensive human resource and payroll system through the use of a commercial off-the-shelf software platform configured for the State by a contractor. SPS is a cloud-based application hosted and operated by a third-party service provider, and is used by numerous State agencies to record personnel transactions, such as appointments, promotions, certain salary adjustments, and for the recordation and maintenance of time and leave transactions and records.

Implementation of SPS was divided into three phases. Phase I was the human resources module, which in November 2014 replaced the former automated human resource processes (personnel transaction system) maintained by DBM. Phase II included timekeeping, calculation of gross payroll, and leave administration, and was fully implemented in October 2016. This Phase replaced the various time processing systems used by participating State agencies. Phase III is intended to provide a comprehensive employee benefits administration module, and is scheduled for statewide implementation in calendar year 2019. As of June 30, 2018, approximately $73.3 million had been paid to the contractors hired for implementation and use of the software system.

We conducted a separate review of the application controls over SPS and matters related to its implementation, and a separate report was issued dated March 7, 2019.

[1] Certain Executive Branch agencies, primarily the Maryland Department of Transportation and the University System of Maryland, maintain their own personnel systems and related policies.

Health Care Benefits Administration

The State provides health care benefits for its employees and retirees (including their spouses and dependents). Below is a description of the benefits and the base period covered by the current contracts.

- Health care coverage for employees and retirees (including their spouses and dependents) is provided through three major insurance providers that administer preferred provider organization (PPO), exclusive provider organization (EPO), and integrated health model (IHM) plans. Mental health care coverage is included in these health care plans. The current contracts cover the period from August 14, 2014 to December 31, 2020.

- Dental insurance is provided through two plans offered by two separate providers that administer a preferred provider organization (DPPO) and a health maintenance organization (DHMO). The current dental plan contracts are in effect from August 14, 2014 to December 31, 2019.

- Prescription drug coverage is provided through an administrator for which the current contract is in effect from January 1, 2018 to December 31, 2020.

The State directly pays claims for the PPO, EPO, prescription drug plan, and DPPO plans. It self-funds these plans and accepts the risk for all costs associated with these plans. For the IHM and DHMO plans, the State pays an insurance premium to the provider and the provider accepts the risk associated with the benefits. The costs for annual health care benefits have increased from approximately $1.3 billion for fiscal year 2014 to approximately $1.7 billion for fiscal year 2018. Health care enrollment and costs paid in fiscal year 2018 for plan participants, which include State employees, retirees, spouses, dependent children, direct pay participants, and satellite agency participants (such as covered employees of local governments) are summarized in Table 1.

Table 1
Plan Participants in the State of Maryland's Health Benefits Programs and the Related Costs for Fiscal Year 2018

Plan Type	Enrollment (as of January 1, 2018)	Dollar Claims Paid	Administrative Expenses Paid	Premiums Paid	Total Payments
PPO	55,478	$396,163,272	$20,305,380	N/A	$416,468,652
EPO	63,714	593,123,596	23,274,752	N/A	616,398,348
IHM	3,147	N/A	N/A	$20,805,020	20,805,020
POS (Note 1)	228	1,983,209	95,829	N/A	2,079,038
Prescription Drug	115,353	579,203,642	13,697,930	N/A	592,901,572
Dental PPO	97,581	44,472,370	1,526,666	N/A	45,999,036
Dental HMO	14,054	N/A	N/A	3,490,872	3,490,872
Totals	[redacted]	$1,614,946,089	$58,900,557	$24,295,892	$1,698,142,538

Source: OPSB records (unaudited)
N/A – not applicable.
Note 1 – The point of service (POS) plan was available only to members of the State Law Enforcement Officers Labor Alliance (SLEOLA) bargaining unit.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the five findings contained in our preceding audit report dated May 19, 2015. As disclosed in Table 2, we determined that OPSB satisfactorily addressed four of these findings. The remaining finding is repeated in this report.

Table 2
Status of Preceding Findings

Preceding Finding	Finding Description	Implementation Status
Finding 1	Controls were not adequate over the payment of administrative fees for the health care and prescription drug programs.	Not repeated
Finding 2	OPSB did not adequately pursue and resolve the results of an independent audit of the prescription drug program.	Not repeated
Finding 3	OPSB had not established a formal policy to ensure the timely initiation and completion of participant eligibility reviews.	Not repeated
Finding 4	OPSB inappropriately stored sensitive personally identifiable information in clear text.	Not repeated
Finding 5	Internal controls were not sufficient to ensure that all collections were deposited.	**Repeated** (Current Finding 4)

Findings and Recommendations

Payroll Adjustments

Finding 1
The Office of Personnel Services and Benefits (OPSB) had not provided guidance to certain agencies regarding the need to establish controls over manual payroll adjustments nor had it established adequate internal procedures for ensuring that it processed only properly authorized payroll adjustments.

Analysis
OPSB, as the control agency for the Statewide Personnel System (SPS), had not provided formal guidance to agencies using SPS regarding the risks associated with manually processed payroll adjustments and the need to establish sufficient control procedures. In addition, OPSB had not established and documented its own procedures for ensuring that it accepted and processed only properly authorized adjustments from user agencies. According to SPS records, OPSB processed 11,555 payroll adjustments manually submitted by user agencies in calendar year 2017, resulting in pay increases of approximately $5.7 million, and pay decreases of approximately $700,000.

Employee payroll adjustments, such as retroactive pay adjustments, were manually compiled by user agencies and submitted each pay period to OPSB for processing on SPS. These adjustments are manually calculated and submitted, outside of the automated time recording and payroll processing within SPS and, therefore, are riskier transactions. However, OPSB had not informed agencies of this risk and the need to establish appropriate procedures to ensure their propriety. During our recent audits of State agencies that have implemented SPS for payroll processing, we have noted and reported on certain State agencies that lacked adequate controls over such payroll adjustments. To date we have reported that two agencies could not document that manually prepared payroll adjustments had been reviewed by independent supervisory personnel for propriety, and the agencies did not use available SPS reports to confirm that only authorized adjustments had been processed by OPSB. As the State agency responsible for SPS implementation and operation, OPSB should provide guidance to user agencies on implementing and maintaining such controls in the SPS environment.

Furthermore, OPSB had not developed internal procedures for ensuring and documenting that only properly authorized adjustments were accepted and processed in SPS. OPSB management advised us that OPSB maintained a listing of authorized user agency personnel as a reference to ensure that only authorized

adjustments were accepted for processing; however, we found that the listing was not available to all OPSB personnel responsible for processing adjustments. In addition, OPSB's verifications that the adjustments had been appropriately authorized were not documented and there was no procedure to ensure that only user agency authorized adjustments were ultimately processed.

Recommendation 1
We recommend that OPSB

a. **establish formal guidance for agencies using SPS to assist those agencies with the design and implementation of controls for ensuring that only valid and authorized payroll adjustments are submitted to and processed by OPSB, and**
b. **establish and document internal procedures for ensuring that only authorized adjustments are accepted from user agencies and processed.**

Health Care Benefits Administration System

Background
OPSB uses its Benefits Administration System (BAS) to support the administration of employee health care benefits, including the enrollment of new employees into plans and changes to employee elected benefit coverage. According to OPSB, as of June 30, 2018, BAS supported the provision of health care benefits for approximately 259,000 active employees, retirees, and other participants, such as satellite participants from local governments, and their dependents.

The BAS database contains health insurance and prescription drug program eligibility and insurance premium payment records, including sensitive personal information (names, addresses, social security numbers, and dates of birth), for participants and their dependents. When fully implemented, Phase III of SPS will replace certain primary functions and applications of BAS; nevertheless, BAS will continue to be used for certain fiscal applications. According to its records, OPSB processed health benefit disbursements totaling approximately $1.7 billion in fiscal year 2018.

Finding 2
Certain critical adjustments could be processed in BAS by OPSB staff without independent review and approval.

Analysis
OPSB had not established procedures to ensure the propriety of certain critical transactions to add individuals in BAS to enroll for benefits as "direct pay" individuals. Direct pay individuals include, for example, COBRA participants who pay OPSB directly for insurance premiums rather than through payroll deduction. OPSB had no procedure, such as an independent on-line approval requirement or the independent verification of output reports to supporting documentation, to ensure the propriety of these transactions.

In addition, the 25 OPSB employees who required this access, either in a primary or back-up capacity, could also void invoices submitted to these individuals. These employees were in a position, therefore, to improperly enroll individuals in benefits and void the associated invoices without detection. According to OPSB's records, 1,685 participants were added to BAS under the direct pay category during calendar year 2017. Also, according to OPSB records, during calendar year 2017 insurance premium invoices totaling $20 million were voided on BAS.

Recommendation 2
We recommend that OPSB establish procedures, such as an independent verification of output reports, to ensure that all transactions to add direct pay individuals to BAS or void invoices are subject to review and approval by independent supervisory personnel, and that this review be documented.

Finding 3
OPSB did not adequately monitor employee access capabilities on BAS, and certain employees had unnecessary critical access.

Analysis
OPSB did not adequately monitor employee access capabilities on BAS to ensure that access was properly restricted. OPSB advised us that a periodic review of user access was performed to ensure that OPSB employee access granted was appropriate. However, there was no documentation of such reviews and we noted that certain employees had system access that they did not need. Specifically, of the 31 employees we examined with some level of critical access, 6 had access to make changes to health benefit information, such as to add dependents to the system, even though these employees did not require the access to perform their job duties.

The State of Maryland *Information Security Policy* requires agencies to monitor the controls over their information systems, including periodic reviews of employee access for propriety.

Recommendation 3
We recommend that OPSB

a. **perform documented periodic reviews for propriety of employee access to BAS as called for by the aforementioned *Information Security Policy*; and**
b. **take any necessary corrective action as a result of these reviews, such as removing access from OPSB employees who do not require such access to perform their normal job duties, including the six employees noted in our finding.**

Cash Receipts

Finding 4
Internal controls were not sufficient to ensure that all collections were deposited.

Analysis
Controls were not sufficient over cash receipts collected directly by OPSB (excluding lockbox collections), which totaled approximately $147.1 million during the audit period, according to OPSB's records. OPSB's collections consisted primarily of checks for prescription drug rebates and premium payments for State health insurance paid by certain participants, such as local governments and their covered employees.

Our review disclosed that one of the two employees responsible for performing the verifications of the initial record of collections to the subsequent bank deposits was not independent, since the employee had access to the safe where the collections were stored prior to deposit. Our test of 15 checks received at OPSB's office totaling $13.7 million disclosed that, for 8 of the checks totaling $13.1 million, the deposit verification was performed by this employee. In addition, this employee, along with two other employees with access to cash receipts, had the capability to manually post payments to the automated accounts receivable records. Although OPSB advised us that periodic reviews of these manual entries were performed by supervisory personnel, one of these two employees performed the reviews. Furthermore, there was no documentation of the reviews performed.

Under these conditions, there was a lack of assurance that all collections initially received were deposited. A similar condition regarding employees with access to

collections was commented upon in our preceding audit report. Additionally, a similar condition regarding the capability to manually post payments to the automated records without independent supervisory review and approval was commented upon in our two preceding audit reports.

The Comptroller of Maryland's *Accounting Procedures Manual* requires that the reconciliation of cash receipts to deposit be performed by an employee independent of the cash receipts functions. The *Manual* also requires the segregation of cash handling duties from accounts receivable record keeping duties.

Recommendation 4
We recommend that OPSB

a. **ensure that deposit verifications are performed by an employee who does not have access to collections,**
b. **segregate the duties of processing cash receipts and maintaining accounts receivable records (repeat), and**
c. **establish documented independent supervisory review and approval of manual payment entries to the automated accounts receivable records (repeat).**

We advised OPSB on accomplishing the necessary separation of duties using existing personnel.

Information Systems Security and Control

Background
OPSB utilizes the following Department of Information Technology (DoIT) information technology (IT) support services:

- network firewalls and IT security services (such as firewall and intrusion detection prevention systems operations and maintenance)
- IT service desk assistance
- hardware support
- software support (including malware protection support)

OPSB also uses the DoIT-operated statewide network services for connections between its Baltimore site and the Annapolis DBM headquarters location. OPSB and DoIT maintain key OPSB applications and critical supporting data including health insurance coverage files.

Finding 5
Sensitive personally identifiable information (PII) maintained by OPSB was stored without adequate safeguards.

Analysis
Controls over sensitive PII maintained by OPSB were not sufficiently comprehensive to protect this data. Specifically, individual files containing PII pertaining to various health insurance vendors were stored in clear text. For example, we determined that, as of May 31, 2018, one such file contained 44,338 unique social security numbers stored in clear text along with names and dates of birth. Although this data resided on an encrypted hard drive subject to controlled user access, scenarios exist whereby the data could be improperly accessed at the clear text file level, and, accordingly be compromised. We therefore concluded that this sensitive PII was not adequately protected by other substantial mitigating controls.

Sensitive PII is commonly associated with identity theft. Accordingly, appropriate information system security controls need to exist to ensure that this information is safeguarded and not improperly disclosed. The State of Maryland *Information Security Policy* states that confidential data should be protected using encryption and/or other substantial mitigating controls.

Recommendation 5
We recommend that OPSB

a. determine if it is necessary to retain this PII, and delete all unnecessary PII; and
b. in conjunction with DoIT, ensure that necessary PII is itself properly protected by encryption or other substantial mitigating controls.

Finding 6
OPSB lacked assurance that all necessary information technology security and operational controls existed over its flexible spending account system which was hosted, operated, and maintained by a third-party service provider.

Analysis
OPSB lacked assurance that all necessary information technology security and operational controls existed over its flexible spending account system which was hosted, operated, and maintained by a third-party service provider, under a contract dated July 6, 2016 to provide services for State employee health care and dependent care spending accounts. As required by the contract, the service

provider's most recent (at the time of our audit) independent service auditor's report, referred to as System and Organization Controls (SOC) 2 Type 2 review, was performed for the period of January 1, 2017 to December 31, 2017.

The related report, covering the security, availability, processing integrity, and confidentiality trust service principles was issued on April 30, 2018, and was obtained by OPSB. Our June 2018 review disclosed that the SOC report did not address several key security controls necessary for the flexible spending account system that are typically included in a SOC 2 review covering the security and availability principles. For example, the SOC review did not test controls related to restricting connections with untrusted network environments; retention and review of audit logs recording privileged or unauthorized access, system exceptions, or, information security events; and, implementation of data loss prevention software.

The American Institute of Certified Public Accountants has issued guidance concerning examinations of service organizations. Based on this guidance, service organizations (like the aforementioned service provider) may contract for an independent review of controls and the resultant independent auditor's report is referred to as a SOC report. There are several types of SOC reports, with varying scope and levels of review and auditor testing. One type of report, referred to as a SOC 2 Type 2 report, includes the results of the auditor's review of controls placed in operation and tests of operating effectiveness for the period under review and could include an evaluation of system security, availability, processing integrity, confidentiality, and privacy.

Recommendation 6

We recommend that OPSB

a. **ensure that the independent security reviews for its flexible spending account system and related SOC reports address all relevant and necessary security controls, and**
b. **ensure that the service provider implements any critical recommendations made in these reports.**

Audit Scope, Objectives, and Methodology

We have conducted a fiscal compliance audit of the Department of Budget and Management (DBM) – Office of Personnel Services and Benefits (OPSB) for the period beginning April 16, 2014 and ending September 7, 2017. The audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

As prescribed by the State Government Article, Section 2-1221 of the Annotated Code of Maryland, the objectives of this audit were to examine OPSB's financial transactions, records, and internal control, and to evaluate its compliance with applicable State laws, rules, and regulations.

In planning and conducting our audit, we focused on the major financial-related areas of operations based on assessments of significance and risk. The areas addressed by the audit included OPSB's payment of State employees and retirees health insurance and prescription drug benefit claims, monitoring of health care and prescription drug benefit administrators, monitoring prescription drug discounts and rebates, processing of personnel and payroll transactions for certain State agencies, information system security, and cash receipts. We also determined the status of the findings contained in our preceding audit report.

Our audit did not include certain support services provided to OPSB by the DBM – Office of the Secretary. These support services (such as payroll and procurement) are included within the scope of our audit of the Office of the Secretary.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, observations of OPSB's operations, and tests of transactions. Generally, transactions were selected for testing based on auditor judgment, which primarily considers risk. Unless otherwise specifically indicated, neither statistical nor non-statistical audit sampling was used to select the transactions tested. Therefore, the results of the tests cannot be used to project those results to the entire population from which the test items were selected.

We also performed various data extracts of pertinent information from the State's Financial Management Information System (such as revenue and expenditure

data) and the State's Central Payroll Bureau (payroll data). These extracts are performed as part of ongoing internal processes established by the Office of Legislative Audits and were subject to various tests to determine data reliability. We determined that the data extracted from these sources were sufficiently reliable for the purposes the data were used during this audit.

In addition, we extracted data from the Statewide Personnel System and the Benefits Administration System for the purpose of selecting test items, such as new hires and rate changes, and for assessing user access. We performed various tests of the relevant data and determined that the data were sufficiently reliable for the purposes the data were used during the audit. Finally, we performed other auditing procedures that we considered necessary to achieve our audit objectives. The reliability of data used in this report for background or informational purposes was not assessed.

OPSB's management is responsible for establishing and maintaining effective internal control. Internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability of financial records; effectiveness and efficiency of operations, including safeguarding of assets; and compliance with applicable laws, rules, and regulations are achieved.

Because of inherent limitations in internal control, errors or fraud may nevertheless occur and not be detected. Also, projections of any evaluation of internal control to future periods are subject to the risk that conditions may change or compliance with policies and procedures may deteriorate.

Our reports are designed to assist the Maryland General Assembly in exercising its legislative oversight function and to provide constructive recommendations for improving State operations. As a result, our reports generally do not address activities we reviewed that are functioning properly.

This report includes findings relating to conditions that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect OPSB's ability to maintain reliable financial records, operate effectively and efficiently, and/or comply with applicable laws, rules, and regulations. Our report also includes findings regarding significant instances of noncompliance with applicable laws, rules, or regulations. A less significant finding was communicated to OPSB that did not warrant inclusion in this report.

The response from DBM, on behalf of OPSB, to our findings and recommendations is included as an appendix to this report. As prescribed in the

State Government Article, Section 2-1224 of the Annotated Code of Maryland, we will advise DBM regarding the results of our review of its response.

APPENDIX

MARYLAND
DEPARTMENT OF
BUDGET & MANAGEMENT

LARRY HOGAN
Governor
BOYD K. RUTHERFORD
Lieutenant Governor

DAVID R. BRINKLEY
Secretary
MARC L. NICOLE
Deputy Secretary

May 6, 2019

Mr. Gregory A. Hook, CPA
Legislative Auditor
Office of Legislative Audits
State Office Building, Room 1202
301 West Preston Street
Baltimore, Maryland 21201

Dear Mr. Hook:

The Department of Budget and Management (DBM) has reviewed your draft audit report on the DBM - Office of Personnel Services and Benefits for the period beginning April 16, 2014 and ending September 7, 2017. As requested, attached are our responses to the findings in the report.

If you have any questions or need additional information, you may contact me at 410-260-7041 or Joan Peacock, Audit Compliance Unit Manager, at 410-260-7079.

Sincerely,

David R. Brinkley
Secretary

cc: Secretary Michael G. Leahy, DoIT
Marc Nicole, Deputy Secretary, DBM
Brent Bolea, Principal Counsel
Cindy Kollner, Executive Director, OPSB
Catherine Hackman, Deputy Executive Director, OPSB
Anne Timmons, Director, Employee Benefits Division, OPSB
Joan Peacock, Manager, Audit Compliance Unit, DBM

Department of Budget and Management
Office of Personnel Services and Benefits (OPSB)
Response to Legislative Audits Findings and Recommendations
May 2019

Finding 1
The Office of Personnel Services and Benefits (OPSB) had not provided guidance to certain agencies regarding the need to establish controls over manual payroll adjustments nor had it established adequate internal procedures for ensuring that it processed only properly authorized payroll adjustments.

Recommendation 1
We recommend that OPSB

a. establish formal guidance for agencies using SPS to assist those agencies with the design and implementation of controls for ensuring that only valid and authorized payroll adjustments are submitted to and processed by OPSB, and

b. establish and document internal procedures for ensuring that only authorized adjustments are accepted from user agencies and processed.

DBM OPSB Response 1:

We agree with the recommendations as follows:

a. OPSB is in process of developing written guidance to agencies for submitting properly authorized payroll adjustments. The guidance will include the following:

- Instructions for properly completing and submitting payroll adjustment forms with two agency authorized signatures.
- OPSB already maintains a list of agency personnel authorized to submit and approve payroll adjustments. However, procedures for notifying OPSB of updates to the list (e.g., when there is a change in personnel at the agency) will be included in the guidance.
- Requirements that agencies run SPS reports of payroll adjustments prior to submission and after completion of payroll by OPSB. These reports are to be reviewed by supervisory personnel independent of the payroll adjustments process and these reviews will be documented and maintained.

b. OPSB is in process of developing internal procedures for properly processing agency payroll adjustments. The procedures will include the following:

- Steps for reviewing and ensuring that agency requests for payroll adjustments are properly authorized. OPSB will document and maintain its review.

- OPSB will continue to maintain its list of agency personnel authorized to submit and approve payroll adjustments. In addition, OPSB will establish rules for updating the list when there are changes in agency-authorized personnel.
- Each pay period an SPS report will be generated that includes all payroll adjustments. This report will be independently reviewed by supervisory personnel independent of the payroll adjustments in the Personnel Services Division. This review will be documented and maintained.

Finding 2
Certain critical adjustments could be processed in BAS by OPSB staff without independent review and approval.

Recommendation 2
We recommend that OPSB establish procedures, such as an independent verification of output reports, to ensure that all transactions to add direct pay individuals to BAS or void invoices are subject to review and approval by independent supervisory personnel, and that this review be documented.

DBM-OPSB Response 2:

OPSB agrees with the finding, however, OPSB does have certain controls in place, including an independent review to ensure the propriety of critical adjustment transactions. This includes requiring supporting documentation for every transaction, independent review of adjustments transactions and a review of various error reports (e.g., single individual with family coverage). With regard to direct pay and voiding of invoices specifically mentioned in the finding, please note the following:

- The direct pay category includes COBRA participants, contractual employees, special circumstance retirees, and employees on certain leaves of absence. Enrollment or adding these individuals (as a direct pay) requires supporting documentation and, often, additional verifications. For example, contractual employees cannot be enrolled in benefits unless employment is verified through the agency or the Central Payroll Bureau. Additionally, all enrollment transactions, including adding a direct pay individual, are subject to the independent verification and review. Additional procedures were implemented as part of this process to ensure that verifications are appropriately documented. The enrollment auditor verifies not only that the data was keyed in correctly but that the transaction is proper and that supporting documentation was submitted with the batch. No transactions are processed without supporting documentation.

- In the event an invoice should be voided, typically due to receiving additional information after a transaction is processed, documentation is placed in the day's batch of transactions. Further, the BAS will not allow an invoice to be voided without a note placed in the system providing the reason.

The existing internal controls and review process have served to minimize risk. We are not aware of any instances of fraudulent enrollment or improper posting of adjustments to accounts (i.e., voiding of invoices).
While these controls have minimized risk, we understand the audit finding that not all critical adjustment transactions processed by OPSB on the BAS may be subject to review. We have requested a monthly BAS report detailing any instances of voided payments and unapplied invoices. We anticipate receiving the first such report in May 2019. This report will be reviewed by independent supervisory personnel in order to validate all authorized transactions. Such reviews will be documented and maintained.

Finding 3
OPSB did not adequately monitor employee access capabilities on BAS, and certain employees had unnecessary critical access.

Recommendation 3
We recommend that OPSB

a. perform documented periodic reviews for propriety of employee access to BAS as called for by the aforementioned *Information Security Policy*; and
b. take any necessary corrective action as a result of these reviews, such as removing access from OPSB employees who do not require such access to perform their normal job duties, including the six employees noted in our finding.

DBM-OPSB Response 3:

OPSB agrees with the finding as follows:

a. Effective 8/31/2018, EBD instituted a documented process whereby on a monthly basis, the Assistant Directors of each unit review the access levels and user changes in their respective areas. The monthly access report reviewed is initialed and dated by the individual who performed the review. The report is sent to the Internal Audit unit to be maintained.

b. As a result of the above mentioned review, action to correct any improper access identified will be taken within the month identified. A review of everyone's access within BAS, including the six employees noted in the finding, has been completed and access has been adjusted accordingly

to match each employee's respective duties. Documented monthly reviews will continue from this point forward.

In addition, the Internal Audit unit within Fiscal will perform periodic (i.e., at least quarterly) audits to ensure this process is being maintained and documented.

Finding 4
Internal controls were not sufficient to ensure that all collections were deposited.

Recommendation 4
We recommend that OPSB

a. ensure that deposit verifications are performed by an employee who does not have access to collections,
b. segregate the duties of processing cash receipts and maintaining accounts receivable records (repeat), and
c. establish documented independent supervisory review and approval of manual payment entries to the automated accounts receivable records (repeat).

We advised OPSB on accomplishing the necessary separation of duties using existing personnel.

DBM-OPSB Response 4:
OPSB agrees with this finding as follows:

a. As a result of this finding, a change has been made to ensure that employees performing deposit verifications do not have access to collections, including the Accounting Manager who serves as the backup for this process. In addition to this, the Internal Audit Unit within Fiscal will perform periodic (i.e., at least quarterly) audits to ensure this process is being maintained. Finally, access to the safe has been limited to the Assistant Director – Fiscal Services and the Audit Manager.

b. Effective 8/23/2018, EBD updated the access of the employees noted in the analysis so that they no longer had the ability to manually post payments to the BAS. These individuals were not aware of their ability to void invoices, nor did they know how to void invoices in the BAS. Going forward, access levels and changes will be monitored at least on a quarterly basis by the Assistant Directors within EBD (see response to Finding 3). This review will be documented and maintained.

c. Effective immediately, the review of manual payment posting is now verified by the Accounting Manager. This verification will consist of a daily review of lockbox detail per the bank against

the lockbox deposit file from the BAS. A daily log is maintained and initialed by the Accounting Manager or Assistant Director – Fiscal Services to document this verification. EBD has also requested the development of an output report that identifies all manual payments posted in the BAS. This report will be generated on a periodic basis (e.g., weekly) and reviewed by the Accounting Manager. We anticipate these procedures to be implemented in May 2019. As an additional check, the Internal Audit unit has been tasked with performing a random audit of this verification process to ensure EBD remains in compliance with this new policy.

Information Systems Security and Control

Finding 5
Sensitive personally identifiable information (PII) maintained by OPSB was stored without adequate safeguards.

Recommendation 5
We recommend that OPSB

a. determine if it is necessary to retain this PII, and delete all unnecessary PII; and
b. in conjunction with DoIT, ensure that necessary PII is itself properly protected by encryption or other substantial mitigating controls.

DBM OPSB-DoIT Response 5:
We agree with recommendations as follows:

a. OPSB will work with DoIT to determine the most cost efficient approach to perform an inventory of its servers to identify all sensitive PII. This will include the option of procuring a solution that will be able to perform an automated scanning for PII. Based on the results of PII identified, OPSB will determine if it is necessary to retain this PII and will delete all unnecessary PII.

b. OPSB will work with DoIT to ensure that all necessary retained PII is properly protected by use of an approved encryption algorithm, or, other substantial mitigating controls.

As stated by the auditors in their analysis, this data (files identified in the analysis) resided on an encrypted hard drive subject to controlled user access. The following mitigating controls currently exist:

- These files reside on the virtual servers, which are encrypted using an approved encryption algorithm.
- These files are stored in a folder where access is controlled and limited.

Even though these specific "flat-files" are not encrypted at rest, in discussions with DoIT personnel, who are subject matter experts on encryption, it is their view that these mitigating controls are sufficient for protecting PII. However, OPSB is open to further discussions with DoIT on determining if the specific files can be encrypted without any significant negative effect on applications.

Finding 6
OPSB lacked assurance that all necessary information technology security and operational controls existed over its flexible spending account system which was hosted, operated, and maintained by a third-party service provider.

Recommendation 6
We recommend that OPSB

a. ensure that the independent security reviews for its flexible spending account system and related SOC reports address all relevant and necessary security controls, and
b. ensure that the service provider implements any critical recommendations made in these reports.

DBM OPSB-DoIT Response 6:
We agree with recommendations as follows:

a. OPSB's EBD obtained the SOC 2 Type 2 report for its flexible spending account (FSA) system, but due to staffing shortages, did not thoroughly review the report. Going forward, EBD will obtain and review the SOC 2 reports for its FSA system on a timely basis. This review will include a review of the audit opinion as well as an assessment to determine if all necessary controls have been addressed. For any security controls not addressed in the SOC reviews, EBD will advise its FSA service provider and request that future reviews include those controls not verified or tested. EBD has been in touch with the FSA service provider to request that their SOC 2 review covering plan year 2018 include the additional controls noted in the finding that were not tested for plan year 2017.

b. As part of the review of the SOC 2 reports, EBD will ensure that exceptions and any critical recommendations made in the SOC 2 report have been addressed by a corrective action plan developed by the FSA service provider.

Documentation will be maintained for all reviews and follow-up actions noted above.

AUDIT TEAM

Michael J. Murdzak, CPA
Audit Manager

Richard L. Carter, CISA
Information Systems Audit Manager

Nelson W. Hopkins, CPA
Evan E. Naugle
Senior Auditors

Matthew D. Walbert, CISA
Information Systems Senior Auditor

Stephanie A. Laciny
Kush C. Patel
Staff Auditors