Special Review

Statewide Personnel System

Review of the Design and Implementation of Automated Controls

March 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.

The Department of Legislative Services does not discriminate on the basis of age, ancestry, color, creed, marital status, national origin, race, religion, gender, gender identity, sexual orientation, or disability in the admission or access to its programs, services, or activities. The Department's Information Officer has been designated to coordinate compliance with the nondiscrimination requirements contained in Section 35.107 of the Department of Justice Regulations. Requests for assistance should be directed to the Information Officer at 410-946-5400 or 410-970-5400.

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Victoria L. Gruber
Executive Director

Gregory A. Hook, CPA
Legislative Auditor

March 7, 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 review of the Department of Budget and Management's (DBM) Statewide Personnel System (SPS) application controls, as well as matters related to the recent implementation of that system. SPS is the State's software platform for human resources and payroll applications.

We concluded, for the application controls reviewed for the State's recently implemented SPS, the controls were generally adequate to safeguard payroll-related processing. For the 55 business processes that we deemed critical and reviewed, we found that rules had generally been established in a way to minimize risk and restrict access to critical data and functions only to necessary user roles. We also validated the salary data within SPS to confirm that proper salary scales were being used for all job classifications in SPS. Specifically, we reconciled the salary information from SPS as of October 20, 2017 to the approved salary data as of January 1, 2014 from the State's previous human resources processing system, accounting for cost-of-living adjustments and other approved salary changes during the period.

However, our review did disclose that employee personally identifiable information (PII) was not adequately restricted for some users of this system. We identified 36 active user roles within SPS that permitted access to PII. After our inquiry on the matter of PII access, DBM identified 237 employees within 5 of those user roles that provided them with access to PII, even though this access was not required for their job duties.

We also determined that DBM had not established sufficient procedures to help ensure that user access within SPS was appropriately restricted by the 54 State agencies using SPS. Under certain circumstances, DBM granted

State employee user access to SPS without formal authorization by appropriate agency personnel. As a matter of practice, when an employee with SPS access vacates a position, the access is automatically assigned to the new employee. Given that the job duties may not be identical, a formal request for user access should be submitted by the agency in such situations. DBM had also not established a policy requiring State agencies to periodically review their employee user access, nor had DBM provided agencies with appropriate access reports to enable such reviews.

Finally, 5 of the 55 critical business processes reviewed did not have approval paths or other mitigating controls to ensure data modified were proper and approved. For example, one of these business processes permitted users to modify, without independent review and approval, a critical date that affects the calculation of employee leave earnings.

DBM's response to this review is included as an appendix to this report. We reviewed the response to our findings and recommendations, and have concluded that the corrective actions identified are sufficient to address all issues.

We wish to acknowledge the cooperation extended to us during the review by DBM and its willingness to address the issues and implement appropriate corrective actions.

Respectfully submitted,

Gregory A. Hook

Gregory A. Hook, CPA
Legislative Auditor

Table of Contents

Background Information

Statewide Personnel System (SPS) Overview and Implementation

The Statewide Personnel System (SPS) is an information system administered by the Department of Budget and Management (DBM) that is used by 54 State agencies to process their payroll and human resources transactions. SPS also supports an application for employee benefits for State employees. SPS, which was implemented in three phases, replaced the State's previous human resources processing system (also maintained by DBM), as well as numerous independent time processing systems previously used by the participating State agencies. The goal of SPS was to integrate payroll and human resources functions into a unified information system, allowing for easier user access, better monitoring and controls over user actions, and reduced time spent administering payroll functions at the participating agencies.

The first two phases of the SPS system were implemented prior to the commencement of our review, and the third and final phase was fully implemented after our review was completed.

- Phase 1 is the human resources module that replaced the prior automated human resource processing system maintained by DBM. The human resources module handles transactions such as new employee hires and employee terminations. This phase launched in November 2014.

- Phase 2 is the time and attendance module that handles timekeeping and the calculation of gross payroll, including tracking employee leave balances. This module launched for all participating agencies, excluding one agency, in May 2016. The module launched for this final agency in October 2016.

- Phase 3 is the benefits module that tracks and calculates employee benefits, and will allow employees to process their own enrollment in healthcare benefit plans. This module was functioning on a limited pilot basis during our fieldwork and was launched January 1, 2019 after our review was completed.

The State of Maryland hired a contractor to implement SPS and configure a commercial off-the-shelf software platform to meet the needs of the State's human resources and payroll applications. In December 2013, the State's

Department of Information Technology contracted with a software developer for the implementation and use of the software for a five-year period for approximately $43.9 million, with the option for two five-year extensions, increasing the contract value to $104.6 million. Implementation of SPS was overseen primarily by DBM's Office of Personnel Services and Benefits (OPSB).

The SPS platform is provided as a cloud-based service relying on data centers maintained by the commercial software platform's vendor in multiple geographic locations. However, OPSB is responsible for the ongoing operation and maintenance of SPS. Furthermore, as part of the goal to centralize functionality within SPS, DBM absorbed the human resources and certain payroll functions of several smaller agencies. We were informed by DBM management that DBM absorbed 22 human resources positions from various agencies, of which 10 were retained and continue to be used to support these agencies, 10 were abolished, and 2 were moved to other units within OPSB. As of June 2018, SPS was being used by 54 State agencies for processing the personnel and payroll transactions of approximately 50,000 employees. In accordance with the original SPS implementation plan, certain State agencies, such as the Maryland Department of Transportation and the University System of Maryland, continue to maintain separate personnel and payroll systems.

Information System Security

Application controls refer to security practices included within an information system to ensure its operational integrity, and pertain to individual business or application processes within the information system. For the purposes of this review, properly designed application controls should ensure that (1) data inputs are accurate, complete, and authorized; (2) data are processed as intended and safeguarded; (3) outputs are accurate and complete; and (4) a record is maintained to track the processing of data from input to storage and to the eventual output.

The first two phases of the SPS system addressed two types of inter-dependent transactions and processes – human resources and payroll. Human resources transactions include, but are not limited to, the processes and supporting documents used to hire or terminate an employee, to change an employee's rate of pay, and to transfer an employee between agencies. Human resources transactions are considered proper if employees on the payroll are valid and are being paid the proper rates. Payroll transactions relate to processes that directly influence and control the amount an employee is paid for a specified pay period. These include, but are not limited to, recording and certifying employee hours worked, processing paid and unpaid time off, and processing timekeeping adjustments for prior periods. Payroll transactions are considered proper if employees are paid accurately for all hours actually worked for a specified period.

Within the SPS software platform, application controls are designed to ensure that transactions are processed properly by authorized individuals, and include business process controls and user access controls. A well-controlled SPS process should include both user roles that are adequately restricted and limited to appropriate personnel, and business processes that are designed to limit access to modify critical data to appropriate users and that enforce adequate independent approvals, where appropriate. SPS application controls are highly customizable and, accordingly, these controls can be modified by DBM as security or business operations warrant.

Within SPS, a business process is a set of tasks defined by rules that direct how a transaction is processed. Business process rules, which reflect decisions to be made on transaction processing, include enforcing restrictions on who can initiate a transaction type and who can approve the transaction at various points in the process. These rules also dictate which data fields and personnel records are modified, and apply error validation rules to help ensure the accuracy of transactions being processed. A particular business process may also launch other business processes and may be used to notify users with important roles within the process of the occurrence of high-risk transactions.

For example, the business process for submitting employee time worked and leave used (the “Enter Time” process) contains system rules or logic (such as approval paths) that will route work time submitted by an employee to the employee’s supervisor for approval. Once the supervisor approves the time, the process is complete.

User access controls within SPS include, but are not limited to a “supervisory organization” assignment and a user “role.” User access controls define how users are permitted to interact with SPS, including which records a user can see and modify. The assignment of a user to a “supervisory organization” restricts which groups of employees the user has access to, as defined by the applicable “supervisory organization,” which could be an entire State agency or a unit within that agency. The user’s role also defines what actions the user can take within the supervisory organization, such as viewing certain information and processing certain types of transactions, and what reporting tools are available to the user.

There are numerous user roles in SPS. Two roles significant to our review are the Timekeeper role and the Timekeeper Approver role. The Timekeeper role is responsible for recording employee time and leave data into SPS, such as from an employee's timesheet, for employees who may not have access to a computer to record their time directly. The Timekeeper Approver role is responsible for approving such transactions for each employee.

While all State employees using SPS and their supervisors have access to SPS to record or approve time records, as applicable to their position, there were 1,942 users as of December 5, 2017 that were assigned 4,831 other critical roles.

Employee Complaints After Certain Agencies Transitioned to SPS

In October 2016, personnel in certain State agencies raised concerns about potential underpayments after those agencies transitioned to SPS. We discussed this matter with DBM management in January 2017 as part of this application control review, and we were advised that they were aware of these concerns. DBM identified three agencies affected by this issue, but advised that the vast majority of the problems were concentrated within one agency that had delayed its transition to SPS for payroll/timekeeping until October of 2016. DBM stated that similar problems occurred at two other agencies, but on significantly smaller scales.

DBM management advised us that a substantial number of pay discrepancies resulted from manual data entry errors and high-volume workloads for timekeepers and timekeeper approvers, particularly at this agency. Specifically, many of this agency's employees were shift personnel and, because they had no access to computer terminals, these shift employees recorded their actual work time on paper logs, which was later entered into SPS by designated timekeepers. This situation was believed to be worsened by the fact that these employees frequently earned overtime and shift differential pay, creating the need for retroactive pay adjustments. The sheer volume of manual processing for time entry for these employees led to certain processing delays and errors.

DBM management also advised us that corrective action was taken through the agency's implementation of automated biometric time clocks that interface with and post time directly to SPS. According to DBM statistics, this corrective action was successful in reducing the opportunity for errors because work time was automatically recorded and there was a reduced need for retroactive manually processed pay adjustments. As of May 2017, we were advised that automated time clocks were in place in all the agency's facilities.

We analyzed the volume of the agency's retroactive pay adjustments using SPS records for the period from January 1, 2017 through July 31, 2017 to assess the impact of these corrective actions. As noted in the table below, the number and value of pay adjustments decreased significantly in May 2017 after the biometric time clocks were implemented. This trend held steady through July 2017, the last month for which we obtained data. Based on these results, we believe that it is reasonable to conclude that these corrective actions were generally successful and resulted in reducing the number of manual adjustments required and, consequently, the potential for errors in processing those adjustments.

Aforementioned Agency's Adjustments to Pay

Month	Total Number of Payroll Adjustments	Total Dollar Value of Payroll Adjustments
January 2017	1,961	$377,013
May 2017	212	$ 99,497

Source: DBM records

Review Scope, Objectives, and Methodology

Scope and Objectives

We conducted an application control review to evaluate the reliability of the automated system controls within the Statewide Personnel System (SPS). SPS is the State of Maryland's software platform for human resources and payroll applications. The scope of our review included the human resources (Phase 1) and time and attendance (Phase 2) modules that had been implemented in 54 State agencies at the time our review commenced. The scope of our review did not include the benefits module (Phase 3), which was launched on January 1, 2019.

The objectives of our review were to

1. document and assess the appropriateness of current system controls including user access, over certain critical transactions to ensure the proper functioning of the SPS payroll and human resources applications; and

2. validate the salary data within SPS to confirm that proper salary scales were being used for all job classifications in SPS.

Methodology

To complete our first objective, we determined, based on our professional judgement, that 55 of the 86 total active business processes as of April 25, 2018 were critical (such as transactions that change employee pay data, change employment status, or affect time and leave records). We reviewed the system controls and business process rules for these 55 business processes. In making this determination, we first obtained an understanding of the 86 active processes with the aid of the Department of Budget and Management (DBM). The identity of the 55 processes selected for review were shared with DBM, which generally agreed with our assessment of their critical nature.

Our review was primarily concerned with two types of automated controls — user access to system capabilities and business process controls — that govern the steps the associated transactions must take to be completed, including transaction approval paths. For the purposes of this review, we considered a transaction to have adequate approval paths when initiating users were adequately restricted, independent approvals were required from appropriate user types at the appropriate time(s) in a transaction's processing, and any additional context-sensitive system logic routed transactions to appropriate individuals within a user group if needed. For example, if the routine approver for a transaction also initiated the transaction, an adequate approval path would require the system to find an alternate approver or backup approver.

Our review consisted of discussions with DBM personnel, direct inspection of system configurations within SPS, and substantive testing of transactions processed through the system to validate our conclusions in this area. In addition, we reviewed the reported results of the System and Organization Controls (SOC 2 Type 2) review of the underlying software platform conducted by an independent accounting firm for the period November 1, 2015 through September 30, 2016 and for the period October 1, 2016 through September 30, 2017. We conducted other procedures as we deemed necessary to achieve our objectives.

For our second objective, we reconciled the salary information from SPS as of October 20, 2017 to the approved salary data as of January 1, 2014 from the State's previous human resources processing system, accounting for cost-of-living adjustments and other approved salary changes during the period.

This review did not examine or comment on any separate manual controls that may exist, either centrally at DBM or at agencies using SPS. The review of such controls is subject to audit during our fiscal compliance audits of the applicable State agencies.

Our review did not constitute an audit conducted in accordance with generally accepted government auditing standards. Had we conducted an audit in accordance with generally accepted government auditing standards, other matters may have come to our attention that would have been included in this report.

Our review was conducted primarily during the period from March 2017 through December 2017, and certain information was updated as of April 2018. DBM's response to this application control review 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.

System and Organization Controls (SOC) Review

The software platform's vendor obtained, from an independent accounting firm, a SOC review of the software platform that is shared by all platform customers, including the State of Maryland. The exact scope and level of such reviews may vary. In this case, the firm prepared a SOC 2 Type 2 report. This type of system security report includes the results of the firm's review of controls placed in operation and tests of operating effectiveness for the period under review, including its data center used by the State.

While not a specific audit objective, due to the significance of the software platform to SPS, we performed a detailed review of the report for the period from November 1, 2015 through September 30, 2016. We concluded that the review's scope provided adequate assurance that the underlying infrastructure and State data were adequately secured. We also obtained the SOC 2 Type 2 report issued for the period from October 1, 2016 through September 30, 2017. For both reports, we noted that the independent auditor did not identify any material control weaknesses in the design and sufficiency of the software developer's internal controls.

Findings and Recommendations

Conclusions

Based solely on the work we conducted and the processes in place at the time of our review, we concluded that application controls for the State's recently implemented Statewide Personnel System (SPS) appeared to be adequately designed and implemented. Further, we concluded that the risk for significant payroll irregularities appeared to be mitigated by those automated controls in place at the time of our review, and with the understanding that they were functioning as designed and intended. The conclusions contained in this review are not intended to provide future assurance regarding the adequacy of those processes reviewed, which are subject to modification by the Department of Budget and Management (DBM).

Specifically, for the 55 business processes that we reviewed, we concluded that rules, such as approval paths, had been established in a way that appeared to minimize risk and restrict access to critical data and functions only to necessary user roles. Except for certain business processes as described on page 16, we also determined that these business processes had adequate approval paths established which, if adhered to, would provide adequate assurance that the related transactions were independently reviewed and approved. Although the description of each of the processes we reviewed are not included in this report, we did share our findings about the specific 55 business processes with DBM during the course of our review.

In addition, we found that all salary data within SPS were valid and accurate. Finally, we identified certain areas for improvement with respect to user access reviews and authorizations. Certain users were granted access to SPS without formal authorization by agency personnel, and DBM had not established a policy requiring agencies to periodically review SPS user access. In addition, we noted that adequate safeguards were not in place to restrict access to sensitive personally identifiable information (PII) for State employees. Specifically, 237 employees were assigned to 5 user roles with access to PII which was not needed for their job duties.

User Access

Background

DBM is responsible for processing critical user access requests for the SPS. State agencies using SPS submit SPS access request forms that create new user access capabilities for their employees. Specifically, user access controls define how users are able to interact with SPS, including the records they may view and data they may modify (via the transactions they can initiate and/or approve). As of December 5, 2017, there were approximately 50,000 State employees on SPS, and 4,831 role assignments in SPS held by 1,942 users with critical access. For the purposes of this review, we defined "critical access" as an employee's ability to process transactions within SPS that affect payroll or human resources records other than their own.

Finding 1

DBM did not perform a comprehensive review to ensure that access to all PII for State employees stored in SPS was properly restricted to employees who needed this access for their job duties.

Analysis

DBM had not conducted a comprehensive review to ensure that access to PII within SPS was restricted to only employees who needed it for their job duties. We identified 36 active user roles within SPS that permitted assigned users to view employee social security numbers (SSNs) in the employee profiles within their assigned supervisory organizations. We discussed the necessity of PII access for these 36 user roles with DBM during our review. After our discussion, DBM determined that, as of September 2018, 5 of the 36 user roles (with 237 assigned employees) had PII access that was not needed for the related employees to perform their job duties.

Each employee in SPS is assigned a unique identification number (worker number) which is not considered PII. However, each employee's profile also includes personnel information including the employee's name, address, employee performance evaluations, and education, as well as employee SSNs, which are often displayed in plain text on numerous SPS screens. DBM advised us that certain user roles require access to employee SSNs because of necessary interaction with other State agencies, such as the Central Payroll Bureau (CPB) and the State Retirement Agency (SRA), that use SSNs as the only unique identifiers in their automated systems. For example, SPS timekeepers must use employee SSNs to identify employee pay records on CPB reports to routinely review and reconcile overtime and other payments between SPS and CPB.

After our inquiry and review, DBM subsequently advised us that it had removed access to PII from the aforementioned five user roles. In our opinion, this condition highlights the need for DBM to periodically ensure that PII in SPS is as limited as practicable, and that access to PII recorded in SPS is restricted to employees who require it for their job duties.

State law defines any record containing an individual’s name combined with a SSN as PII. The State of Maryland *Information Security Policy* states that this information must be restricted only to users who require it to perform their job duties.

Recommendation 1

We recommend that DBM

a. perform a periodic review to ensure that PII stored in SPS is properly restricted to those user roles for which it is required and delete its access from user roles where it is found to be unnecessary, and

b. take steps to mask SSNs from user view to the extent practicable.

Finding 2

DBM granted certain State employee user access to SPS without formal authorization by agency personnel. In addition, DBM had not established a policy requiring agencies using SPS to periodically review user access for propriety.

Analysis

DBM had not established sufficient procedures to help ensure that user access within SPS was appropriately restricted. Under certain situations, DBM granted State employee user access to SPS without formal authorization by appropriate personnel at the employee’s agency. Furthermore, DBM had not established a policy requiring agencies to periodically review SPS user access for their employees to ensure each employee’s user access was necessary and did not result in incompatible duties.

<u>Certain user access was granted by DBM without agency authorization</u>

Under certain situations, DBM granted State employee user access to SPS without formal authorization by appropriate personnel at the respective agency. Typically, DBM processed requests for new or revised user access based on an authorization for SPS access request form submitted by appropriate agency personnel. However, under DBM’s policy at the time of our review, when an employee with SPS access vacated his or her position at the agency, the next employee assigned to that position was automatically assigned the same user access held by the former employee. In other words, a new properly approved authorization form was not required from the agency nor expected by DBM. While it is reasonable to assume that, in many instances, the new employee would require the same level of access, this may not always be the case. A new authorization for SPS access request form should be required as a means to assess employee access needs and to control and account for access granted.

During our review of user access granted in March 2018, we identified 73 vacant employee positions within 24 agencies that had been assigned one or more critical SPS user roles. As of August 3, 2018, 27 of these positions had been filled and the new employees had the same user access as the former employees. We did not evaluate the propriety of the user access granted in these 27 instances.

<u>Periodic agency review of user access was not required by DBM</u>
DBM had not established a policy requiring agencies to periodically review SPS user access for their employees to ensure each employee's user access is necessary and does not result in incompatible duties. Furthermore, DBM had not created an SPS report that captures each user's access that could be periodically provided to or produced by agencies to facilitate this review. Periodic reviews of SPS access granted to employees would help ensure that access to perform critical functions and sensitive data in SPS is properly restricted and controlled.

The State of Maryland *Information Security Policy* requires agencies to monitor the security controls over their information systems periodically to ensure that the access is strictly controlled and restricted to appropriate personnel. Because DBM would not have specific knowledge of the job duties of every SPS user within an agency, DBM, as the agency responsible for administering SPS, should establish a policy requiring user agencies to perform periodic reviews of their respective employees' user access. The DBM policy should also contain instructions on how to perform this review and DBM should develop any tools necessary for the review.

Recommendation 2
We recommend that DBM

a. **establish a formal procedure requiring that documented State agency authorization for SPS user access request forms be submitted for each employee requiring access,**
b. **establish a formal policy requiring agencies to periodically review SPS user access to ensure that user access granted to each of their employees is necessary and proper, and**
c. **provide agencies with appropriate reports of access granted to employees at their agencies to facilitate user access reviews.**

Business Processes

Finding 3
Certain critical business processes did not have approval paths established.

Analysis

Certain critical business processes did not have established approval paths to ensure that data modified through the business processes were proper and independently approved. In other words, one employee could unilaterally modify potentially critical SPS data.

We identified 55 business processes in SPS as of April 2018 as critical to the functioning of human resources or payroll processes. Examples include the *Hire* process, which adds new employees to the payroll, and the *Enter Time* process, which allows employees to enter their actual work time for processing in SPS (in place of a traditional timesheet). Of these 55, we determined that 5 lacked adequate approval paths, and sufficient compensating controls did not exist to mitigate the risk posed by the lack of approval paths. For example, one business process permitted users to modify, without independent review and approval, a critical date that affects the calculation of employee leave earnings. Another business process allowed users to move workers to a different supervisory organization, which would prevent the worker from appearing on an agency's SPS reports, preventing supervisory review of the access granted to the worker. Consequently, there was a lack of assurance that data processed through these 5 business processes were proper.

For 26 of the remaining 50 business processes, while we determined that approval paths were not present, sufficient mitigating system controls did exist to reduce the risk of improper transactions. Finally, for the remaining 24 business processes, we determined that sufficient approval paths existed to ensure that transactions were subject to independent supervisory review and approval.

As the agency responsible for administering SPS, DBM was responsible for establishing the automated controls for the system's business processes. We shared the results of our review of all 55 business processes with DBM. DBM management agreed that approval paths had not been established for some business processes during the implementation of SPS. DBM advised us that approval paths generally were established only for those processes related to and for which a corresponding approval requirement existed in law or regulation. As evidenced by our review, and as agreed to by DBM, other business processes exist in SPS that are deemed to be critical to ensuring the proper processing of human resources and payroll transactions.

Recommendation 3

We recommend that DBM review business processes in SPS for which no approval paths exist, and establish approval paths or other mitigating controls, as necessary, to ensure independent review and approval of critical data and transactions processed.

APPENDIX

MARYLAND

DEPARTMENT OF
BUDGET & MANAGEMENT

LARRY HOGAN
Governor

BOYD K. RUTHERFORD
Lieutenant Governor

DAVID R. BRINKLEY
Secretary

MARC L. NICOLE
Deputy Secretary

March 1, 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 special review of the Design and Implementation of Automated Controls related to Statewide Personnel System, administered primarily by DBM - Office of Personnel Services and Benefits. 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: Marc Nicole, Deputy Secretary, DBM
Brent Bolea, Principal Counsel
Cindy Kollner, Executive Director, OPSB
Catherine Hackman, Deputy Executive Director, OPSB
Leslie Buchman, Director, Shared Services, 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
Special Review of the Design and Implementation of Automated Controls of the Statewide Personnel System
February 2019

Finding 1
DBM did not perform a comprehensive review to ensure that access to all PII for State employees stored in SPS was properly restricted to employees who needed this access for their job duties.

Recommendation 1
We recommend that DBM

a. perform a periodic review to ensure that PII stored in SPS is properly restricted to those user roles for which it is required and delete its access from user roles where it is found to be unnecessary, and
b. take steps to mask SSNs from user view to the extent practicable.

DBM OPSB Response 1:

We agree with the recommendations.

a. DBM OPSB agrees to re-evaluate user roles periodically to ensure that PII stored in SPS is properly restricted to those user roles for which it is required. Specifically, such evaluations will be performed after final implementation (of Phase 3) in July 2019 and, going forward, when there are any significant changes made to or that affect the SPS. Where determined unnecessary, we will delete a user roles' access to PII.

b. DBM OPSB will review the possibility of masking SSNs from user view in the SPS and will take appropriate action to the extent practicable.

Department of Budget and Management
Office of Personnel Services and Benefits (OPSB)
Response to Legislative Audits Findings and Recommendations
Special Review of the Design and Implementation of Automated Controls of the Statewide Personnel System
February 2019

Finding 2
DBM granted certain State employee user access to SPS without formal authorization by agency personnel. In addition, DBM had not established a policy requiring agencies using SPS to periodically review user access for propriety.

Recommendation 2
We recommend that DBM

a. establish a formal procedure requiring that documented State agency authorization for SPS user access request forms be submitted for each employee requiring access,

b. establish a formal policy requiring agencies to periodically review SPS user access to ensure that user access granted to each of their employees is necessary and proper, and

c. provide agencies with appropriate reports of access granted to employees at their agencies to facilitate user access reviews.

<u>DBM OPSB Response 2:</u>

We agree with the recommendations.

a. As the auditor brought these issues to the attention of DBM OPSB, additional measures were established to address the issues noted, specifically that of 'inheriting' access of another employee. Currently, SPS user access request forms are required to be submitted for access to SPS. These forms will be maintained for audit verification purposes.

   It is important to note that the inheritance process in SPS is something that cannot be changed within the system. However, most support positions have mandatory training required and related to their position. Access to the SPS is not provided until the training has been completed. As an added control, training will not be assigned until the SPS user access request form has been received. This additional control will help to ensure user roles are appropriately assigned.

b. DBM OSPB implemented procedures that require HR Directors or their designee to review quarterly reports of SPS user access. Per the review procedures, the review should be completed within 30 days of receipt and will be conducted to ensure that all user access granted to employees at their agencies is necessary and proper. Agencies are required to document their review and maintain records for audit verification purposes. After review, agencies are required to submit an OPSB Security Form to Shared Services to remove any access levels determine improper or not needed. These quarterly reviews began January 2019.

c. For these quarterly reviews, DBM OPSB created a new report to provide detailed information on access granted to employees by agency. Beginning January 2019, DBM OPSB will generated and send these reports quarterly to HR Directors or their designee for the quarterly reviews of user access (mentioned in the response to Recommendation 2b). In addition, agencies may request this report on an ad-hoc basis, as needed. Separately, agencies may also run an access report within SPS to review individual security roles.

Department of Budget and Management
Office of Personnel Services and Benefits (OPSB)
Response to Legislative Audits Findings and Recommendations
Special Review of the Design and Implementation of Automated Controls of the Statewide Personnel System
February 2019

Business Processes

Finding 3
Certain critical business processes did not have approval paths established.

Recommendation 3
We recommend that DBM review business processes in SPS for which no approval paths exist, and establish approval paths or other mitigating controls, as necessary, to ensure independent review and approval of critical data and transactions processed.

DBM OPSB Response 3

We agree with the recommendation. As mentioned in the audit analysis, our aim, as part of the SPS Project, was to require approval paths with business processes where there was a related or corresponding approval required by law or regulation. During the implementation of SPS, we reviewed each event in order to determine whether an approval path was appropriate and necessary.

As clarification, there is a difference between business process and task in SPS. Some events identified as a business process by the auditors are actually Tasks. These events were configured as Tasks and do not have approval steps. Tasks are set up to stand-alone and cannot be assigned an approval path. In order to establish an approval path, an event would have to change from a Task to a Business Process with separate steps that could include establishing an approval path.

Of the 55 events identified by the auditors, DBM agreed to perform an additional review of five events to determine any possible improvements, including the reconsideration of whether an approval path is necessary and appropriate. Four of these five events are currently Tasks. Thus, this review will include determination of whether the Task should be re-established as a Business Process that could include steps, such as an approval path. Resources will be available to start this additional review in April 2019.

Audit Team

Michael J. Murdzak, CPA
Audit Manager

Evan E. Naugle
Senior Auditor

Christopher J. Fowler
Staff Auditor