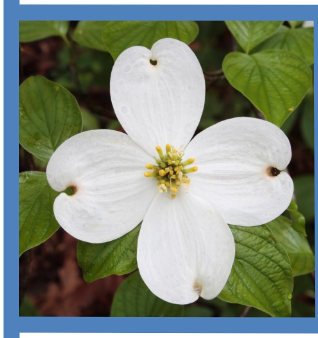

STATE COMPENSATION BOARD

INTERNAL CONTROL QUESTIONNAIRE REVIEW RESULTS AS OF JULY 2018

Auditor of Public Accounts
Martha S. Mavredes, CPA
www.apa.virginia.gov
(804) 225-3350

- TABLE OF CONTENTS -

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

November 5, 2018

Robyn de Socio, Executive Secretary
State Compensation Board
102 Governor Street
Richmond, VA 23219

INTERNAL CONTROL QUESTIONNAIRE REVIEW RESULTS

We have reviewed the Internal Control Questionnaire, completed on July 19, 2018, for the **State Compensation Board** (Compensation Board). The purpose of this review was to evaluate if the agency has developed adequate internal controls over significant organizational areas and activities and not to express an opinion on the effectiveness of internal controls. Management of Compensation Board is responsible for establishing and maintaining an effective control environment.

The Auditor of Public Accounts has developed a new process for auditing agencies that are not required to have an audit every year, which we refer to as "cycled agencies." Traditionally, we audit these agencies at least once every three years. We now employ a risk-based approach to auditing the cycled agencies. Under this approach, annually we will perform a risk analysis for all of the cycled agencies considering certain criteria and divide the agencies into two pools. One pool will receive an annual audit and the other pool will be subject to review in a special project focused on one area of significance as well as a review of internal controls in the form of a questionnaire. All agencies will undergo an Internal Control Questionnaire review at least once every three years. This letter is to communicate the results of the Internal Control Questionnaire review.

Review Process

During the review, the agency completes an Internal Control Questionnaire that covers significant organizational areas and activities including payroll and human resources; revenues and expenses; procurement and contract management; and information technology and security. The questionnaire focuses on key controls over these areas and activities.

We review the agency responses and supporting documentation to determine the nature, timing, and extent of additional procedures. The nature, timing, and extent of the procedures selected depend on our judgment in assessing the likelihood that the controls may fail to prevent and/or detect events that could prevent the achievement of the control objectives. The procedures performed target risks or business functions deemed significant and involve reviewing internal policies and procedures. Depending on the results of our initial procedures, we may perform additional procedures including reviewing evidence to ascertain that select transactions are executed in accordance with the policies and procedures and conducting inquiries with management. The "Review Procedures" section below details the procedures performed for Compensation Board. The results of this review will be included within our risk analysis process for the upcoming year in determining which agencies we will audit.

Review Procedures

Due to the implementation of the new statewide accounting system, we reviewed system access and a selection of system and transaction reconciliations in order to gain assurance that the statewide accounting system contains accurate data. The definitive source for internal control in the Commonwealth is the Agency Risk Management and Internal Control Standards (ARMICS) issued by the Department of Accounts; therefore, we also included a review of ARMICS. The level of ARMICS review performed was based on judgment and the risk assessment at each agency. At some agencies only inquiry was necessary; while others included an in-depth analysis of the quality of the Stage 1 Agency-Level Internal Control Assessment Guide, or Stage 2 Process or Transaction-Level Control Assessment ARMICS processes. For the Compensation Board we reviewed documentation supporting Stage 1 and Stage 2.

We reviewed the Internal Control Questionnaire and supporting documentation detailing policies and procedures. As a result of our review, we performed additional procedures over the following areas: expenses, revenues and information system security. These procedures included validating the existence of certain transactions; observing controls to determine if the controls are designed and implemented; reviewing transactions for compliance with internal and Commonwealth policies and procedures; and conducting further review over management's risk assessment process.

As a result of these procedures, we noted areas that require management's attention. These areas are detailed in the "Review Results" section below.

Review Results

We noted the following areas requiring management's attention resulting from our review:

- Compensation Board has formal, documented policies and procedures over its monthly financial system reconciliations and is performing the reconciliations in accordance with Commonwealth Accounting Policies and Procedures Manual Topic 20905. However, we noted the reconciliations do not include evidence of management's review and approval. Management should ensure all reconciliations contain sufficient evidence including the preparer's signature and completion date, as well as the reviewer's signature and approval date.

- Compensation Board does not review the Cancelled Record Report from the Commonwealth's human resource system, as required by the Department of Accounts Payroll Bulletin 2015-06 and the Virginia Retirement System Employer Manual. Compensation Board should regularly review the report to ensure employee information properly interfaces and is accurately recorded in the retirement system. In addition, management should ensure this report is incorporated in its formally documented procedures for the monthly payroll and retirement reconciliations.

- We observed the following information system security related deficiencies:

  - Compensation Board is in the process of creating, documenting, and implementing a comprehensive Information Technology (IT) Security Policy applicable to the agency's IT environment to govern its IT Security Program and establish controls over both sensitive and non-sensitive information systems, but the policy is in draft form and is incomplete. Management should complete the formalized IT Security Policy to ensure compliance with the Commonwealth's Information Security Standard, SEC 501, (Security Standard), Section 1.4, and address the issues noted below. Once completed, management should evaluate the current risk management and contingency documentation to ensure the documents align with the requirements in the newly implemented IT Security Policy and the Security Standard.

  - Compensation Board does not secure the database that supports three sensitive systems in accordance with the Security Standard and industry best practices. We were unable to determine based on Compensations Board's documentation if these systems were mission critical. The Security Standard requires, and industry best practices, such as the Center for Internet Security, recommend implementing specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability. We communicated certain control weaknesses to management in a separate document marked Freedom of Information Act Exempt under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. By not meeting the minimum requirements in the Security Standard and recommendations in industry best practices, Compensation Board cannot ensure the confidentiality and integrity of data within these sensitive systems. Management should evaluate the best way to secure their sensitive data and configure the sensitive systems according to best practices and the minimum security requirements in the Security Standard. In addition, management should evaluate which systems are mission critical and ensure this is clearly documented.

  - Compensation Board has not conducted an IT security audit of its sensitive systems within the last three years. Compensation Board plans to complete IT security audits over all sensitive systems during February 2019, using the IT audit services from Virginia Information Technologies Agency. Section 1.4 of the Security Standard requires that IT systems containing sensitive data, or that reside in a system with a sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall receive an IT security audit at least once every three years. Management should complete the planned IT security audits over each sensitive system to test the effectiveness of controls, comply with the Security Standard requirements and to help ensure the protection of sensitive and mission critical data.

We discussed these matters with management on October 31, 2018. Management's response to the findings identified in our review is included in the section titled "Agency Response." We did not validate management's response and, accordingly, cannot take a position on whether or not it adequately addresses the issues in this report.

This report is intended for the information and use of management. However, it is a public record and its distribution is not limited.

Sincerely,

Deputy Auditor of Public Accounts

JDE/clj

TYRONE NELSON
CHAIRMAN

ROBYN DE SOCIO
EXECUTIVE SECRETARY

CRAIG BURNS
MARTHA MAVREDES
EX-OFFICIO MEMBERS

COMMONWEALTH OF VIRGINIA

Compensation Board
P.O. Box 710
Richmond, Virginia 23218-0710

November 30, 2018

MEMORANDUM

TO: Staci Henshaw, Deputy Auditor of Public Accounts

SUBJECT: Agency Response to Internal Control Questionnaire Review Results

Thank you for the opportunity to review your preliminary Results Letter to the Compensation Board regarding the Internal Control Questionnaire Review for the fiscal year ended June 30, 2017 and to respond to the results noted in the report. The review results noted three items requiring management attention.

Formal, documented policies and procedures over monthly financial system reconciliations include a management review process. Although policies and procedures are followed during these reconciliations, the sample tested did not include the sign-off initials of management on paperwork documentation. This was an oversight during the period where the agency was transitioning from the old CARS to the new Cardinal statewide accounting system utilizing new reporting tools, and in the transition to a new Fiscal Officer following the retirement of the agency's long-serving former fiscal officer. The agency will ensure all reconciliations more clearly demonstrate evidence of the review by management.

The auditors identified that formal, documented procedures related to reconciliation of payroll records to retirement system records did not also include a review of the Cancelled Record Report from the Commonwealth's HR system (data maintained by the shared services unit of the Department of Human Resources Management). Incorporation of the Cancelled Record Report into the reconciliation processes has occurred beginning with the reconciliation of records for May, 2018, and review of the report has also been added to the agency's formal, documented procedures related to this monthly reconciliation process.

The auditors have also noted deficiencies related to information system security; two of the noted items relate to the current process of documenting a comprehensive IT security policy within the agency, and the need for audit of the IT systems. As noted in the letter of results, the Compensation Board is nearing the end of its review and establishment of a comprehensive IT security policy that has been ongoing for several months, and the IT systems security audit is scheduled for February, 2019. The third item relates to security of databases supporting sensitive systems. While the results letter states that there is a database supporting three sensitive systems that is not secured in accordance with the Security Standard and industry best practices, the agency notes that there are two separate databases, where each supports a sensitive system. The third database is no longer categorized as sensitive. This third database had been previously identified as sensitive, but during the current process to document a comprehensive IT security policy, this system has been updated to reflect that it is not sensitive. This change was made after the auditor's review.

While the other two database systems are secured, the Compensation Board is pursuing options to enhance this security in accordance with the Security Standard and industry best practices, to be further evaluated with the IT system security audit scheduled for February, 2019.

Please let me know should you have any additional questions or need further information.

Sincerely,

Robyn M. de Socio
Executive Secretary

cc: Compensation Board Members
Charlene Rollins, Customer Service Manager
Kim Jezek, Fiscal Officer
Dan Munson, Assistant IT Director
Melanie Morrison, Information Security Officer
Charlotte Lee, Budget Manager
Mark Pellett, Financial & Management Analyst