DEPARTMENT OF HUMAN RESOURCE MANAGEMENT

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2017

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

AUDIT SUMMARY

Our audit of the Department of Human Resource Management (Human Resource Management) for the fiscal year ended June 30, 2017, found:

- proper recording and reporting of all transactions, in all material respects, related to the Health Insurance Fund, the Local Choice Health Care Fund, and the Worker's Compensation Fund;

- matters involving internal control and its operation necessary to bring to management's attention;

- instances of noncompliance with applicable laws and regulations or other matters that are required to be reported; and

- one comment to management related to Human Resource Management's pending implementation of a new accounting standard for accounting and reporting of postemployment benefits other than pensions.

–TABLE OF CONTENTS–

COMMENT TO MANAGEMENT

Other Post Employment Benefit Reporting Changes

In June 2015, the Governmental Accounting Standards Board (GASB) issued Statement No. 75, *Accounting and Financial Reporting for Postemployment Benefits Other Than Pensions.* This accounting standard becomes effective for fiscal year 2018 and covers participating employer accounting and reporting of postemployment benefits other than pensions (OPEB).

Human Resource Management administers the Commonwealth's Pre-Medicare Retiree Healthcare Program, which is considered an OPEB plan subject to the GASB standard. Under the standard, the Commonwealth will report OPEB liabilities as employees earn benefits by providing services. The GASB standard allows the Commonwealth to offset the OPEB liabilities by the assets it has accumulated to fund the benefits; however, this offset is currently not possible for the Pre-Medicare Retiree Healthcare Program, as it operates on a "pay as you go" basis and; therefore, has no accumulated assets. There will also be a significant increase in the required financial statement disclosures for the Commonwealth and participating agencies discussing the OPEB plans.

As the OPEB administrator, Human Resource Management is responsible for disseminating the appropriate financial information and required disclosures to all participating entities for inclusion in the participant's individual financial statements. Human Resource Management plans to rely heavily on the work of its actuary to prepare the necessary accounting and reporting information related to GASB Statement No. 75. The actuary currently prepares a valuation report related to the Commonwealth's Pre-Medicare Retirees. Human Resource Management should continue to work closely with its actuary to ensure the fiscal year 2018 valuation report is prepared in accordance with GASB Statement No. 75, and made available to all participating agencies in a timely manner. Human Resource Management should also ensure that staff are adequately trained and prepared to answer inquiries received from participating agencies during the implementation process.

Along with administering the health benefits for Commonwealth employees, Human Resource Management administers the Local Choice (TLC) health benefits program, which provides coverage to local jurisdictions, including options for pre-Medicare retiree benefits. Human Resource Management should assess the TLC program and work with the participating localities to determine how the GASB Statement No. 75 OPEB valuation and reporting will be performed.

The implementation of GASB Statement No. 75 for fiscal year 2018 will not only impact Human Resource Management, but also all participating agencies and localities. Each participating entity will be required to report their share of the OPEB liability in their individual financial statements, along with increased disclosures related to the Pre-Medicare retiree program. Successful implementation of GASB Statement No. 75 is critical to ensure all participating entities have the necessary accounting and reporting information to prepare their individual financial statements.

AUDIT FINDINGS AND RECOMMENDATIONS

The Department of Human Resource Management (Human Resource Management) collects, manages, and stores Commonwealth data related to compensation, benefits, and employee leave balances. Due to the sensitivity of this data, management must implement the necessary controls to ensure the confidentiality, integrity, and availability of the data within the various systems. Human Resource Management should obtain the necessary resources, and continue working with the shared services provided by the Virginia Information Technologies Agency (VITA), to develop and implement an agency-wide security plan. Our review of information system security resulted in the following five recommendations to management, which resulted in part from the need to allocate additional resources to information security.

Improve Web Application Security Controls

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes
Previous Title: Improve System Security for the Time, Attendance, and Leave System

Human Resource Management continues to not implement certain minimum security controls for a web application used for employee time tracking as required by the Commonwealth's Information Security Standard, SEC501 (Security Standard), and industry best practices. Lacking application and database controls can create vulnerabilities that expose data to potential compromises and system unavailability, which, as a result, may lead to reputational damage and financial penalties imposed on Human Resource Management.

We communicated the specific control weaknesses and compliance references to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under §2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. In general, the weaknesses relate to system activity monitoring and configuration of the web application.

The weaknesses identified in the FOIAE document continue to persist in Human Resource Management's environment due to limited and constrained information security resources. Additionally, Human Resource Management relies on a third party service provider to implement some of the required controls. Human Resource Management should obtain the resources necessary and collaborate with its third party service provider to remediate the concerns identified in the FOIAE recommendation. Remediating these weaknesses will help to protect the confidentiality, integrity, and availability of data in the application environment.

Improve IT Risk Management and Disaster Recovery Planning
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Partial

Human Resource Management continues to lack certain components of an established information technology (IT) risk management and disaster recovery planning (DRP) process in accordance with the Security Standard. Our review of Human Resource Management's IT risk management and DRP controls identified the following weaknesses.

- Human Resource Management continues to not evaluate or determine if the data stored in its mission essential and sensitive systems are subject to regulatory requirements, as required by the Security Standard (*Security Standard section: 4.2 IT System and Data Sensitivity Classification*). Evaluating and documenting the regulatory requirements will assist Human Resource Management to comply with applicable regulations.

- Human Resource Management continues to lack IT system baseline configurations for any of its mission essential and sensitive systems. Baseline configurations serve as a basis for system builds, changes to information systems, as well as information about specific system components that reflect the current enterprise architecture. By not having baseline configurations in place for its mission essential and sensitive systems Human Resource Management increases the risk that systems will not be restored in a timely manner in the event of an outage *(Security Standard section: CM-2 Baseline Configuration)*.

- Human Resource Management did not perform a risk assessment for one sensitive system as required by the Security Standard (*Security Standard section: RA-3 Risk Assessment*). Specifically, Human Resource Management changed the classification of a system from non-sensitive to sensitive in March of 2017 but has not conducted a risk assessment for the system. Without completing a risk assessment Human Resource Management may not identify applicable risks to the system and may not implement appropriate mitigation efforts. Human Resource Management did not conduct the risk assessment due to a misunderstanding about the requirements in the Security Standard.

- Human Resource Management does not have a process for performing self-assessments of risk assessments and preparing a report of the self-assessment results, as required in the Security Standard (*Security Standard section: 6.2 Risk Assessment Requirements*). Without a process to perform self-assessments, Human Resource Management cannot verify the continued validity of the risk assessments and IT security threats that may impact Human Resource Management's ability to carry out mission essential functions. Human Resource Management does not have a process for self-assessments due to a lack of IT resources.

Human Resource has made progress since our last audit to remediate certain security weaknesses previously reported, specifically, updating the Business Impact Analysis and IT Systems and

Data Sensitivity Classifications for consistency. However, the weaknesses identified above continue to persist due to limited and constrained IT and security resources. Human Resource Management should evaluate its current IT and security staffing levels, and allocate the resources necessary to implement and enforce the requirements in the Security Standard for IT risk management.

Improve Security Awareness and Training
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes

Human Resource Management continues to lack an effective or reasonable security awareness and training program in accordance with the requirements of the Security Standard. Our review of Human Resource Management's security awareness and training program identified the following weaknesses.

- Human Resource Management continues to not verify that IT systems end users complete basic security awareness training initially and on an annual basis. Specifically, 8 out of 18 (44%) new hires did not complete initial security awareness training in fiscal year 2017. The Security Standard requires that Human Resource Management provide basic security awareness training to all information system users as part of initial training for new users, and at least on an annual basis thereafter *(Security Standard section: AT-2 Security Awareness)*.

- Human Resource Management continues to not provide appropriate role-based (i.e. system owner, data owner, system administrator, and data custodian) security training or document user acknowledgment of role specific responsibilities. Role based security training and responsibility acknowledgement is required for users to fulfill role-based requirements defined in the Security Standard *(Security Standard sections: AT-3 Role-Based Security Training)*.

By not verifying that IT system users and new hires complete security awareness training, Human Resource Management increases the risk that users will not be able to identify security incidents and react appropriately. Additionally, by not designating system specific roles or providing role based training and acknowledgement, Human Resource Management increases the risk that users will not be capable of performing system specific security responsibilities to adequately secure and manage sensitive and mission critical systems.

Human Resource Management has made progress since the last audit to remediate certain weaknesses previously reported, including creating an information security awareness training policy, hiring a training coordinator, and providing some users with annual refresher training. However, the weaknesses still exist because Human Resource Management allocated the training coordinator to other higher priority projects and the agency lacks a comprehensive security awareness training program to

implement the requirements in the training policy. Human Resource Management should allocate the necessary resources to implement and enforce the requirements in the Security Standard related to security awareness and training, including a procedure to verify all new employees complete training in the appropriate timeframe.

Improve Vulnerability Identification and Mitigation Process
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Human Resource Management does not have a process to consistently identify and mitigate system vulnerabilities in accordance with the Security Standard. Specifically, Human Resource Management does not consistently scan sensitive systems at least once every 90 days, does not review the vulnerability scan results, and does not remediate legitimate vulnerabilities within 90 days.

Human Resource Management relies on the Commonwealth's Comprehensive Infrastructure Agreement with Northrop Grumman (NG), also known as the IT Infrastructure Partnership, to perform and complete vulnerability scans. Human Resource Management does not communicate with the IT Infrastructure Partnership to ensure they perform scans at least once every 90 days. In addition, because Human Resource Management does not review scan results, they were unaware the IT Infrastructure Partnership provided incomplete vulnerability scans; therefore, Human Resource Management could not determine if legitimate vulnerabilities exist in the IT environment. Human Resource Management did not provide a cause as to why they are not reviewing the scans and not remediating legitimate vulnerabilities within 90 days.

The Security Standard requires Human Resource Management to conduct vulnerability scans on sensitive systems at least once every 90 days and to remediate legitimate vulnerabilities within 90 days commensurate with risk. *(Security Standard sections: RA-5 & RA-5-COV Vulnerability Scanning)*. Without communicating with the IT Infrastructure Partnership to receive and review vulnerability scans every 90 days, Human Resource Management may not identify significant security weaknesses in sensitive systems that may impact the confidentiality, integrity, and availability of data. In addition, not remediating legitimate vulnerabilities timely increases the risk that a malicious user will exploit a known vulnerability to gain unauthorized access to the system, which could result in a data breach.

Human Resource Management should collaborate with the IT Infrastructure Partnership to ensure that all sensitive systems receive vulnerability scans at least once every 90 days. Additionally, Human Resource Management should allocate the necessary resources to review the scans and remediate legitimate vulnerabilities within 90 days. Improving the vulnerability identification and mitigation process will better enable Human Resource Management to protect the sensitive and mission critical data.

Improve Database and Application Security

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Human Resource Management does not have certain database and application security controls for a sensitive system that performs human resource related functions. The Security Standard and industry best practices define required and recommended security controls to protect the confidentiality, integrity, and availability of data stored in databases and processed by the application.

We communicated the specific control weaknesses and compliance references to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under §2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. In general, the weaknesses relate to system activity monitoring, change management, database configuration, and access management controls.

The weaknesses identified in the FOIAE document exist in Human Resource Management's environment due to limited and constrained information security resources. Additionally, Human Resource Management relies on a third party service provider to implement some of the required database controls. Human Resource Management should obtain the resources necessary and collaborate with its third party service provider to remediate the concerns identified in the FOIAE recommendation. Implementing these security controls will reduce the data security risk and better protect the confidentiality, integrity, and availability of sensitive and mission critical data.

AGENCY HIGHLIGHTS

The Department of Human Resource Management (Human Resource Management) administers the Commonwealth's Personnel Act, health insurance plans for state and local employees, and the workers' compensation program. Human Resource Management's responsibilities include providing expertise in the areas of compensation, equal employment compliance, health benefits, and human resources policy and training. Human Resource Management is also the Commonwealth's central source for information about the Commonwealth's employment work force and provides a listing of state employment opportunities.

The Office of Contracts and Finance (Contracts and Finance) manages all accounting, finance, and procurement activities for Human Resource Management. Contracts and Finance also provides accounting services for the Office of Health Benefits, which administers the health insurance and related benefits.

Health Insurance Fund

The Office of Health Benefits administers the comprehensive health benefits and long-term care programs for state employees, state retirees, and their dependents. It also provides health benefits and long-term care programs to local governments and school jurisdiction employees, dependents and retirees through the Local Choice program. The Comprehensive Annual Financial Report of the Commonwealth presents the activity of these self-insured health benefits program.

Human Resource Management contracts with Anthem Blue Cross and Blue Shield to serve as the administrator for the Commonwealth's statewide standard preferred provider organization (PPO) health plan and the Local Choice health plan. Additionally, Kaiser Foundation Health Plan of the Mid-Atlantic States is contracted to administer the consumer driven health plan. AON Consulting, Inc. provides services to evaluate the actuarial liabilities and reserve requirements of the self-funded health benefits program and the reserve requirements of the Local Choice program.

Workers' Compensation Fund

The Office of Workers' Compensation provides direction to state agencies on workers' compensation, workplace safety and loss control, and return to work programs. The office also determines if the Commonwealth has adequate workers' compensation insurance protection, claims administration, training, and loss control services. The Workers' Compensation Fund provides all state employees with a covered injury sustained in the course and scope of employment with salary and wage protection, medical expenses, and other costs.

The Commonwealth operates a self-insured workers' compensation program administered by Human Resource Management. The Comprehensive Annual Financial Report of the Commonwealth shows the program as a component of the Risk Management Internal Service Fund. Human Resource Management contracts with Managed Care Innovations (MCI) to manage cost containment and claims administration. The Office also contracts with Oliver Wyman to provide an annual actuarial analysis of

the Workers' Compensation Fund. This analysis identifies funding needs and required reserves to meet short and long-term claim obligations.

Information Systems

Human Resource Management's Office of Information Technology (ITECH) manages the Commonwealth's personnel management system. This system consists of a database used for processing and managing personnel, compensation, and health benefits data. The benefits system is a subsystem of the personnel management system that maintains health benefits records on all eligible employees, employee dependents, and participating retirees.

ITECH recently completed a significant system migration. Human Resource Management contracted with an IT services company to assist the migration of the personnel management system from a legacy mainframe to a modern multi-tier platform. The project was completed in the spring of 2017 and includes advanced security features that resolved some of the recommendations identified in the Findings and Recommendations section of previous reports.

In 2012, Human Resource Management designed and implemented a time, attendance, and leave system. This system allows employees to electronically record time worked, submit leave requests, and record leave used. Managers are able to electronically approve time worked and leave submissions. Currently 62 agencies with over 17,000 end users are using the system. The Department of Accounts is in the process of implementing an integrated component of the Commonwealth's accounting and financial reporting system, which will include functionality similar to Human Resource Management's time, attendance, and leave system. During 2018, a subset of the user agencies will begin transitioning to the Commonwealth's integrated system for time and labor tracking. Human Resource Management will continue operation of its time, attendance, and leave system until 2019 when the final user agencies migrate onto the Commonwealth's integrated system.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 15, 2017

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Robert D. Orrock, Sr.
Chairman, Joint Legislative Audit
and Review Commission

We have audited the financial records and operations of the **Department of Human Resource Management** (Human Resource Management) for the year ended June 30, 2017. We conducted this performance audit 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.

Audit Objectives

Our audit's primary objective was to evaluate the accuracy of Human Resource Management's financial transactions as reported in the Comprehensive Annual Financial Report for the Commonwealth of Virginia for the year ended June 30, 2017. In support of this objective, we evaluated the accuracy of recorded financial transactions in the Commonwealth's accounting and financial reporting system, in Human Resource Management's accounting records, and in other information reported to the Department of Accounts; reviewed the adequacy of Human Resource Management's internal control; tested for compliance with applicable laws, regulations, contracts, and grant agreements; and reviewed corrective actions of audit findings from prior year reports.

Audit Scope and Methodology

Management of Human Resource Management has responsibility for establishing and maintaining internal control and complying with applicable laws, regulations, contracts and grant agreements. Internal control is a process designed to provide reasonable, but not absolute, assurance regarding the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws, regulations, contracts, and grant agreements.

We gained an understanding of the overall internal controls, both automated and manual, sufficient to plan the audit. We considered significance and risk in determining the nature and extent of our audit procedures. Our review encompassed controls over the following significant cycles, classes of transactions, and account balances.

Contract procurement	Contract management
Revenues	Claims expenses
Actuary reporting	Financial reporting
Information systems security	

We performed audit tests to determine whether Human Resource Management's controls were adequate, had been placed in operation, and were being followed. Our audit also included tests of compliance with provisions of applicable laws, regulations, contracts, and grant agreements. Our audit procedures included inquiries of appropriate personnel, inspection of documents, records, and contracts, and observation of Human Resource Management's operations. We performed analytical procedures, including budgetary and trend analyses. We also tested details of transactions to achieve our objectives.

A non-statistical sampling approach was used. Our samples were designed to support conclusions about our audit objectives. An appropriate sampling methodology was used to ensure the samples selected were representative of the population and provided sufficient, appropriate evidence. We identified specific attributes for testing each of the samples and when appropriate, we projected our results to the population.

Conclusions

We found that Human Resource Management properly stated, in all material respects, the amounts recorded and reported in the Commonwealth's accounting and financial reporting system, in Human Resource Management's accounting records, and in other information reported to the Department of Accounts for inclusion in the Comprehensive Annual Financial Report for the Commonwealth of Virginia.

We noted certain matters involving internal control and its operation and compliance with applicable laws, regulations, contracts and grant agreements that require management's attention and corrective action. These matters are described in the section entitled "Audit Findings and Recommendations."

Human Resource Management has taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this letter. Human Resource Management is still in the process of taking corrective action with respect to several audit findings reported in the prior year; therefore, we have repeated these findings in the section entitled "Audit Findings and Recommendations."

Exit Conference and Report Distribution

We discussed this report with management on January 30, 2018. Management's response to the findings identified in our audit is included in the section titled "Agency Response." We did not audit management's response and, accordingly, we express no opinion on it.

This report is intended for the information and use of the Governor and General Assembly, management, and the citizens of the Commonwealth of Virginia and is a public record.

AUDITOR OF PUBLIC ACCOUNTS

JMR/clj

COMMONWEALTH of VIRGINIA

SARA REDDING WILSON
DIRECTOR

Department of Human Resource Management

101 N. 14TH STREET
JAMES MONROE BUILDING, 12TH FLOOR
RICHMOND, VIRGINIA 23219
(804) 225-2131
(TTY) 711

February 6, 2018

Martha S. Mavredes, CPA
Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

Dear Ms. Mavredes,

We have reviewed your report on our audit for the fiscal year ending June 30, 2017. We appreciate the APA's recognition that DHRM had proper recording of all transactions, in all material respects, related to the Health Insurance Fund, the Local Choice Health Care Fund and the Worker's Compensation Fund.

We also appreciate the findings and recommendations regarding internal controls and compliance matters. We have responded to specific items related to those under a separate detailed response and continue with our efforts related to them.

DHRM engaged in an agreement with VITA Centralized ISO Services to receive services to document and perform Business Impact Analysis and System Security Plans /Risk Assessments for DHRM's multiple sensitive applications/systems. This engagement allows DHRM to satisfy part of the compliance with Commonwealth's Information Security Standard (SEC501-9) requirements. However, many security needs of DHRM for ensuring full compliance are out-of-scope for this agreement. DHRM understands and appreciates the imperative need to comply with SEC501-9, but DHRM lacks the resources to implement and manage the needed comprehensive IT security program. The efforts on complying with the Standard are a continuous work in progress using the existent IT staff.

Sincere Regards,

Sara R. Wilson
Director, Department of Human Resource Management

An Equal Opportunity Employer

DEPARTMENT OF HUMAN RESOURCE MANAGEMENT

As of June 30, 2017

Sara Redding Wilson, Director

Richard Whitfield, Director
Contracts and Finance

Elizabeth Hurst, Fiscal Officer
Contracts and Finance

Belchior Mira, Director
Information Technology