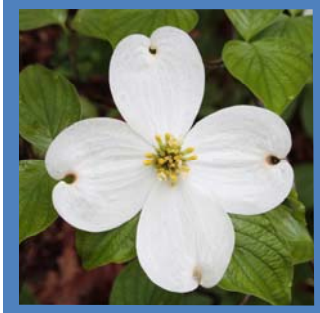

DEPARTMENT OF HUMAN RESOURCE MANAGEMENT

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2016

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 for the fiscal year ended June 30, 2016, 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; and

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

–TABLE OF CONTENTS–

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 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 four recommendations to management.

Improve IT Risk Management and Disaster Recovery Planning – REPEAT

Human Resource Management lacks certain components of an established and reasonable information technology (IT) risk management and disaster recovery planning (DRP) process. The artifacts that comprise an agency's IT risk management and DRP program are essential for protecting IT systems by identifying risks, vulnerabilities, and remediation techniques. Our review of Human Resource Management's IT risk management and DRP controls identified the following weaknesses:

- Human Resource Management continues to not evaluate the data stored in its mission essential and sensitive systems to determine if the data is subject to regulatory requirements, as required by the Commonwealth's Information Security Standard, SEC 501-09 (Security Standard).

- The essential systems inventory and the IT systems and data sensitivity classifications are not consistent. The Security Standard requires that the Information Security Officer verify and validate that all agency IT systems and data have been reviewed and classified as appropriate for sensitivity. Human Resource Management has not adequately defined all sensitive systems within its IT environment. The risk management and assessment process is based on the outputs of the Business Impact Analysis and individual systems sensitivity classifications.

- Human Resource Management continues to not have IT system baseline configurations developed for any of its mission essential and sensitive systems, as required by the Security Standard. Baseline configurations serve as a basis for system builds, releases, and changes to information systems, as well as including information about specific information system components that reflect the current enterprise architecture.

Human Resource Management should allocate the resources necessary to implement and enforce all of the requirements as defined in the Security Standard for IT risk management and disaster recovery planning, as identified above.

Improve Security Awareness and Training – REPEAT

Human Resource Management continues to not implement an effective or reasonable security awareness and training program. The Security Standard requires agencies to train employees annually as to their responsibilities while interacting with sensitive data. An established security awareness and training program is essential in protecting agency IT Systems and data. Our review of Human Resource Management's security awareness and training program identified the following weaknesses:

- Human Resource Management continues to not verify that all end users receive basic security awareness training on an annual basis. The Security Standard requires that Human Resource Management provide basic security awareness training to all information system users on an annual basis, and as part of initial training for all new users. Approximately 20 percent of Human Resource Management staff did not complete annual security awareness training in fiscal year 2016.

- Human Resource Management continues to not provide additional role-based security training, or acknowledgement of responsibilities, for personnel with assigned security roles. Role-based security training is essential for employees and contractors who manage, administer, operate, and design IT systems to ensure that the related individuals are appropriately trained in their roles and responsibilities in protecting Human Resource Management's mission critical sensitive systems and data.

Human Resource Management should improve its security awareness and training program by enforcing the requirement for all employees to complete annual training and providing role-based security training.

Improve System Security for the Time, Attendance, and Leave System – REPEAT

In 2012 Human Resource Management designed and implemented the Time, Attendance, and Leave system (TAL). The TAL system is used by multiple agencies and thousands of end users across the Commonwealth. As the system owner, Human Resource Management must maintain compliance with the Security Standard and industry best practices.

The Security Standard requires implementing specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability. We identified internal control weaknesses and opportunities for improvement based on the Security Standard, that were communicated to management in a separate document marked Freedom of Information Act (FOIA) Exempt under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. Human Resource Management should devote the necessary resources to address the weaknesses identified.

Improve Controls over the Personnel Management Information System – REPEAT

Human Resource Management is the system owner of the Commonwealth's Personnel Management Information System (PMIS). PMIS contains sensitive data, such as employee and benefits records of active and separated Commonwealth of Virginia employees. As the system owner, Human Resource Management must maintain compliance with the Security Standard and industry best practices.

The Security Standard requires implementing specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability. We identified internal control weaknesses and opportunities for improvement based on best practices, that were communicated to management in a separate document marked Freedom of Information Act (FOIA) Exempt under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

Human Resource Management should continue with its efforts to address the weaknesses identified. Additionally, Human Resource Management should continue to obtain exceptions from the Chief Information Security Officer of the Commonwealth for any requirements of the Security Standard that are unable to be implemented due to the legacy nature of PMIS.

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 underwriting oversight 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.

Other Post Employment Benefit Reporting Changes

The Governmental Accounting Standards Board (GASB) issued two new standards related to accounting and reporting for postemployment benefits other than pensions (OPEB). The first is GASB Statement No. 74, *Financial Reporting for Postemployment Benefit Plans Other Than Pension Plans,* which is effective for fiscal year 2017 and covers accounting and reporting of postemployment benefit plans other than pension plans. The second standard is GASB Statement No. 75, *Accounting and Financial Reporting for Postemployment Benefits Other Than Pensions,* which is effective for fiscal year 2018 and covers participating employer accounting and reporting of postemployment benefits other than pensions.

Human Resource Management administers the Commonwealth's Pre-Medicare Retiree Healthcare Program, which is considered an OPEB plan subject to the new GASB standards. Under the new standards, the Commonwealth will report OPEB liabilities as employees earn benefits by providing services. The Commonwealth is allowed to offset the OPEB liabilities by the assets it has accumulated to fund the benefits. 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 be a significant increase in the required financial statement disclosures for the Commonwealth and participating agencies discussing the OPEB plans. Human Resource Management should continue to work with the Department of Accounts to meet all new reporting requirements related to the new GASB standards.

Information Systems

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

ITECH is in the process of a significant system migration. Human Resource Management contracted with an IT services company to assist in migrating PMIS from a legacy mainframe platform to a flexible and modern multi-tier platform. The project was originally estimated for completion by June 30, 2016; however, ITECH experienced delays and has revised the estimated completion to the first quarter of 2017. Human Resource Management anticipates that this new system platform will provide a more robust control structure and address many of the recommendations identified in the Findings and Recommendations section of this report.

In 2012 Human Resource Management designed and implemented the Time, Attendance, and Leave system (TAL). TAL 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 59 agencies with almost 16,000 end users are using TAL.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 16, 2016

The Honorable Terence R. McAuliffe
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, 2016. 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, 2016. In support of this objective, we evaluated the accuracy of recorded financial transactions in the Commonwealth Accounting and Reporting System, Cardinal, and in other information reported to the Department of Accounts; reviewed the adequacy of the Human Resource Management's internal controls; 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 nonstatistical 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 Accounting and Reporting System and Cardinal, as well as other information reported to the Department of Accounts for inclusion in the Comprehensive Annual Financial Report for the Commonwealth of Virginia. The Department records its financial transactions on the cash basis of accounting, which is a comprehensive basis of accounting other than accounting principles generally accepted in the United States of America. The financial information presented in this report came directly from the Commonwealth Accounting and Reporting System and Cardinal.

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 "Findings and Recommendations."

Human Resource Management is still in the process of taking corrective action with respect to audit findings reported in the prior year; therefore, we have repeated these findings in the section entitled "Findings and Recommendations."

Exit Conference and Report Distribution

We discussed this report with management on February 7, 2017. 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/alh

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 9, 2017

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, 2016. 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. Last year in July, DHRM entered into an agreement with VITA Centralized ISO Services to augment DHRM's limited staff performing, documenting, and implementing the requirements established by the Commonwealth's Information Security Standard (SEC501-09). The efforts on complying with the Standard are a continuous work in progress.

Sincere Regards,

Sara R. Wilson
Director, Department of Human Resource Management

DEPARTMENT OF HUMAN RESOURCE MANAGEMENT

(As of June 30, 2016)

Sara Redding Wilson, Director

Richard Whitfield, Director
Contracts and Finance

Elizabeth Hurst, Fiscal Officer
Contracts and Finance

Belchior Mira, Director
Information Technology