DEPARTMENT OF HUMAN RESOURCE MANAGEMENT

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2015

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, 2015, 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 obtain the necessary resources, including but not limited to the hiring of a full-time Information Security Officer, to develop and implement an agency-wide security plan. Our review of information system security resulted in the following four recommendations to management, which resulted in part from the need to allocate additional resources to information security.

Improve IT Risk Management and Disaster Recovery Planning

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 has not evaluated 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, SEC501-09 (Security Standard). Additionally, Human Resource Management has not evaluated the potential damages to the agency and the Commonwealth if the confidentiality, integrity, or availability of mission essential and sensitive data is compromised.

- Human Resource Management has not formally assigned the roles and responsibilities of system owners, data owners, system administrators, and data custodians for its mission essential and sensitive systems, as required by the Security Standard. The personnel assigned to the related roles must also be educated and trained in their respective roles.

- 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 has not performed risk assessments for any of its mission essential and sensitive systems, except the Personnel Management Information System and the Benefits Enrollment System. The Security Standard requires risk assessments for all mission essential and sensitive systems. Risk assessments are essential for all designated mission essential and sensitive systems to adequately identify potential threats to an IT system and the environment in which it operates, determine the likelihood that threats will materialize, identify and evaluate vulnerabilities, and determine the loss impact if one or more vulnerabilities are exploited by a potential threat.

- Human Resource Management does 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

Human Resource Management has not implemented 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 does not have a documented security awareness and training policy. The Security Standard requires Human Resource Management develop a security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, and compliance. Lacking a security awareness and training policy increases the risk that Human Resource Management employees will not consider the related training as mandatory, relevant, or essential.

- Human Resource Management does not require 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 98 percent of Human Resource Management staff did not complete annual security awareness training in fiscal year 2015.

- Human Resource Management does not provide additional role-based security training to personnel with assigned security roles and responsibilities. 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.

We recommend that Human Resource Management improve its security awareness and training program by documenting a policy, requiring all employees to receive annual training, and including role-based security training requirements.

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 information security policies and standards in all IT system activities as defined in section 2.7 of the Security Standard.

The Security Standard requires implementing specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability. Our review also compared the established PMIS policies and controls to other Commonwealth of Virginia information systems that are centrally managed, but used throughout the Commonwealth by other agencies. 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 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.

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 that is 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.

In 2012 Human Resource Management began developing a 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. The pilot agencies began using TAL in April 2013 with additional agencies going on-board between 2013 and 2015. Currently 47 agencies with over 13,000 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 15, 2015

The Honorable Terence R. McAuliffe
Governor of Virginia

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

We have audited the financial records and operations of the **Department of Human Resource Management** for the year ended June 30, 2015. 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 the Department 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, 2015. In support of this objective, we evaluated the accuracy of recorded financial transactions in the Commonwealth Accounting and Reporting System and other information they report to the Department of Accounts, reviewed the adequacy of their 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 the Department of Human Resource Management has responsibility for establishing and maintaining internal control and complying with applicable laws and regulations. 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 the Department'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 the Department's operations. We tested transactions and performed analytical procedures, including budgetary and trend analyses. Where applicable, we compared the Department's policies to best practices and Commonwealth standards.

Conclusions

We found that the Department properly stated, in all material respects, the amounts recorded and reported in the Commonwealth Accounting and Reporting System and in 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 or other information the Department reported to the Department of Accounts.

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

Exit Conference and Report Distribution

We discussed this report with management on January 26, 2016. 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

January 29, 2016

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, 2015. 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 have already initiated efforts related to them. These efforts include the recent acquisition of information security services from a VITA resource to augment DHRM's limited staff and assist us as we implement the requirements in Commonwealth's Information Security Standard (SEC501-09).

Sincere Regards,

Sara R. Wilson

Sara R. Wilson
Director, Department of Human Resource Management

An Equal Opportunity Employer

DEPARTMENT OF HUMAN RESOURCE MANAGEMENT

Sara Redding Wilson, Director

Dan Hinderliter, Director
Office of Contracts and Finance

George Gibbs, CFO
Office of Contracts and Finance

Belchior Mira, Director
Office of Information Technology