DEPARTMENT OF HUMAN RESOURCE MANAGEMENT

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2018

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, 2018, found:

- Proper recording and reporting of all transactions, in all material respects, related to the Health Insurance Fund, the Local Choice Health Care Fund, the Line of Duty Act Fund, and the Workers' Compensation Fund except as noted in the finding entitled "Improve Internal Controls Over Financial Reporting;"

- Six findings involving internal control and its operation necessary to bring to management's attention. Of these findings, one is considered to be a material weakness; and

- Four out of the six findings are also considered to be instances of noncompliance with applicable laws and regulations that are required to be reported.

–TABLE OF CONTENTS–

AUDIT FINDINGS AND RECOMMENDATIONS

Improve Controls Over Financial Reporting
Type: Internal Control
Severity: Material Weakness
Repeat: No

Human Resource Management should strengthen its internal controls over financial reporting. As the administrator of the statewide Pre-Medicare Retiree Healthcare plan, which is part of the Health Insurance Fund, Human Resource Management is responsible for preparing required information established by the Governmental Accounting Standards Board (GASB) necessary for financial reporting. For the fiscal year ended June 30, 2018, we audited Human Resource Management's implementation of GASB Statement No. 75, Accounting and Financial Reporting for Postemployment Benefits Other Than Pensions (OPEB). As an 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. We identified significant errors in the financial schedules, as well as elements of the disclosures and supplemental information that did not meet all requirements of GASB Statement No. 75. The errors identified include the following:

- The employee and demographic data for one agency was incorrectly excluded by the actuary when preparing the OPEB valuation.
- The allocation of the OPEB financial information to the participating agencies incorrectly included one agency that should have been excluded from the allocations.
- Two participating agencies were incorrectly excluded from the employer contributions schedule, and thus were not included in the allocation of the OPEB financial information.
- The counts of active and inactive participants were incorrectly calculated and reported by the actuary in the OPEB valuation report.
- The table used to illustrate the impact of the discount rate sensitivity on the OPEB liability was incorrectly prepared and reported by the actuary.
- Benefit payments to be recorded as deferred outflows of resources were understated by $6.5 million.
- The employer and statewide disclosures and supplemental information did not include all required elements per GASB Statement No. 75

Significant delays in preparing the financial information and required disclosures contributed to these errors. Human Resource Management relies heavily on the actuarial valuation to compile the required information. The existing contract with the actuary was not modified to include the scope of

the new reporting requirements and deadlines. Additionally, Human Resource Management did not formally determine who was responsible for preparing the financial information and required disclosures, and did not establish internal deadlines to ensure all information was prepared in a timely manner.

Further contributing to the errors in the financial information is Human Resource Management's lack of a formal review process of the compiled information. The actuarial valuation report is not properly reviewed by Human Resource Management's staff prior to the preparation of the financial schedules and disclosures. A detailed review of the actuary report is necessary to ensure errors and omissions are identified in a timely manner, and to ensure that Human Resource Management agrees with the assumptions used by the actuary. We consider this to be a material weakness in internal control, as there is a reasonable possibility that a material misstatement of the financial information and required disclosures will not be prevented, detected or corrected on a timely basis.

Human Resource Management should consider modifying the existing contract with the actuary, or procure a new contract, specific to the requirements and deadlines for the annual GASB Statement No. 75 reporting. Additionally, the Health Benefits Services and Contracts and Finance service areas at Human Resource Management should work together to establish a formal review process for the actuary report, the financial information, and the required disclosures. The actuary report and disclosures both contain financial and program specific information that will require the coordination of these two service areas to properly review. Internal deadlines should also be established to allow adequate time to review the information. Finally, Human Resource Management should ensure that staff are adequately trained on the financial reporting requirements in order to properly consider, research, and apply the reporting requirements specific to GASB Statement No. 75 in future years.

Improve IT Security Governance
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Human Resource Management does not have an adequate information technology (IT) security governance structure to manage its information security program and comply with the Commonwealth's Information Security Standard, SEC 501 (Security Standard). Human Resource Management is responsible for managing multiple statewide systems that have a material impact on the Commonwealth's financial operations and require extensive IT resources to secure and meet the requirements in the Security Standard. The lack of an adequate IT security governance structure restricts Human Resource Management's ability to mitigate security weaknesses in their IT environment.

The Security Standard requires the agency to ensure the information security program is maintained, is adequate to protect the agency's IT systems, and is effectively communicated throughout the organization (*Security Standard section: 2.4.2*). Specifically, Human Resource Management has control weaknesses in the following areas:

- Human Resource Management does not have an internal full-time Information Security Officer (ISO) that is independent from IT operations;

- Human Resource Management does not use a separate budget line item to account for information security operations;

- Human Resource Management does not have a strategic plan for information security that provides clear direction, milestones, and metric tracking for the information security program; and

- Human Resource Management does not have a process to periodically review and update information security policies/procedures.

In addition to these control weaknesses, Human Resource Management's inadequate IT security governance structure has contributed to the agency's inability to resolve audit recommendations. Between fiscal years 2014 and 2018, Human Resource Management has been unable to resolve multiple IT security related recommendations, with several recommendations included in four consecutive audit reports.

By not having an adequate IT security governance structure to properly manage Human Resource Management's IT security program, there is increased risk that Human Resource Management will not properly secure sensitive IT resources, which can lead to a breach of sensitive data or system unavailability. Human Resource Management should establish an independent security function, specifically an internal full-time ISO, within the organization and integrate IT security with system operations. To reduce any potential conflicts of interest, the ISO should report directly to the agency head, and not the Chief Information Officer. Additionally, Human Resource Management should evaluate its IT resource levels to ensure sufficient resources are available to implement any IT security governance changes and remediate any control deficiencies. Improving the IT governance structure will help ensure the confidentiality, integrity, and availability of sensitive data.

Improve Web Application Security Controls
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Partial (first issued in fiscal year 2014)

Human Resource Management continues to not implement certain minimum security controls for one of its web applications as required by the Security Standard and industry best practices. Lacking application and database controls can create vulnerabilities that expose data to potential compromises and system unavailability, which may lead to reputational damage and financial penalties imposed on Human Resource Management.

Human Resource Management has corrected one of the weaknesses communicated in the prior year finding; however, other weaknesses still exist. 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 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 to implement some of the required controls. Human Resource Management should obtain the resources necessary and collaborate with the third party 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 (first issued in fiscal year 2015)

Human Resource Management continues to lack certain components of an established 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 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 does not perform self-assessments of risk assessments and prepare a report of the self-assessment results, as required in the Security Standard (*Security Standard Section: 6.2 Risk Assessment Requirements*). By not performing 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 perform self-assessments due to a lack of IT resources.

Human Resource Management has made progress since our last audit to remediate certain security weaknesses previously reported. 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.

Review and Document Service Organization Control Reports of Third-Party Service Providers
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Human Resource Management does not have a sufficient process or formal policy for gaining assurance that third-party service providers have adequate controls related to financial processes and IT security. Human Resource Management outsources certain business tasks and functions to service providers who transmit, process, or store sensitive data and assets.

The Commonwealth Accounting Policies and Procedures Manual (CAPP Manual) Topic 10305 requires agencies to have adequate interaction with providers to appropriately understand the providers' internal control environment. Agencies must also maintain oversight over providers to gain assurance over outsourced operations. Additionally, Section 1.1 of the Security Standard states that agency heads remain accountable for maintaining compliance with the Security Standard for information technology equipment, systems, and services procured from providers, and that agencies must enforce the compliance requirements through documented agreements and oversight of the services provided.

Service Organization Control Reports (SOC reports) provide an independent description and evaluation of the provider's internal controls. Without a formal process for obtaining, reviewing and documenting SOC reports, Human Resource Management cannot ensure that providers' controls are designed, implemented, and operating effectively. Although Human Resource Management maintains a high degree of interactions with most of its providers, management is increasing the Commonwealth's risk that it will not detect a weakness in a provider's environment, which could negatively impact the Commonwealth and its employees.

Based on the testwork we performed, Human Resource Management received six separate SOC reports related to the various service providers; however, there is no documentation related to a review for four of the SOC reports received. Human Resource Management has not allocated proper resources to developing and implementing policies and procedures to review, assess, and document the effectiveness of provider controls reported through SOC reports.

Human Resource Management should develop and implement policies and procedures to obtain, review, assess, and document the effectiveness of provider controls reported through SOC reports. In addition, Human Resource Management should use SOC reports as a component of its oversight activities over its providers to confirm they comply with the requirements outlined in the Security Standard, CAPP Manual, and industry best practices. If the SOC reports detail complementary controls, Human Resource Management should ensure that these controls are documented and implemented at the agency. If control deficiencies are identified in SOC reports, Human Resource Management should determine if additional controls can be implemented at the agency to mitigate the risk until the provider corrects the deficiency. Finally, Human Resource Management should review existing contracts and service provider agreements to determine if additional SOC reports should be obtained.

Reconcile Billing Records for the Line of Duty Act Program
Type: Internal Control
Severity: Significant Deficiency
Repeat: No

Human Resource Management does not reconcile the Line of Duty Act (LODA) billing records to the agency's benefits system. The benefits system is the source of record for all individuals eligible for LODA benefits and includes plan type, membership elections, and premium rates. Benefits received are based on the information within the benefit system; however, LODA billing records are keyed and updated outside of the benefits system. A reconciliation between the two records was not performed for the duration of the fiscal year.

Human Resource Management became responsible for the administration and billing of LODA health benefits starting in fiscal year 2018. Human Resource Management did not identify and address the need for a reconciliation between the LODA billing records and the benefits system. As a best practice, agencies should develop internal policies and procedures that reflect current operations, and agency management should document its approval of these policies and procedures. In addition, best practices indicate that an agency should document, review, and update policies and procedures regularly to ensure the documentation is clear, concise, and adequately address operational risk identified.

A lack of clearly documented policies and procedures increases the risk that reconciliations are not completed or completed inadequately. Inadequate reconciliation of the two records could result in improper billing for LODA benefits. Human Resource Management should develop and implement procedures for reconciling the LODA billing records to the benefits system. The reconciliation should ensure that total number of individuals billed and the monetary amount billed agrees to the benefits system.

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, health benefits plans for the Virginia Line of Duty Act, 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.

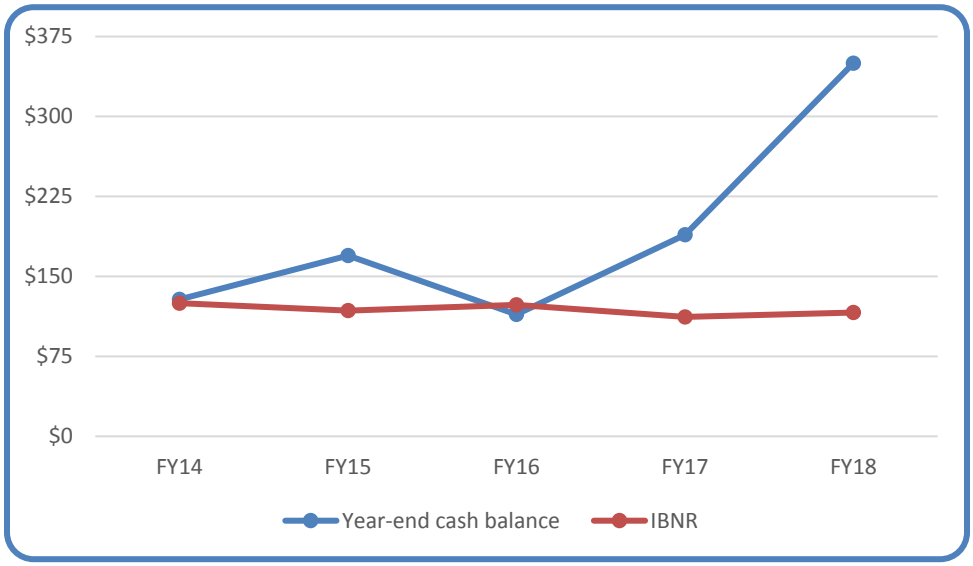
The Contracts and Finance service area within Human Resource Management manages all accounting, finance, and procurement activities for the agency. Contracts and Finance also provides accounting services for the Health Benefits Services and the Workers' Compensation service areas within Human Resource Management. Contracts and Finance contracts with actuaries to perform annual valuations for the Health Insurance Fund, the Local Choice Health Care Fund, the Line of Duty Act Fund, and the Workers' Compensation Fund. The actuarial valuations include an estimate of the incurred but not reported (IBNR) claims for each fund. The IBNR represents the amount owed for valid claims that have not yet been reported as of the fiscal year-end, and is used in the preparation of the Commonwealth's Comprehensive Annual Financial Report.

Health Insurance Fund

Health Benefits Services administers the comprehensive health benefits and long-term care programs for state employees, state retirees, and their dependents. 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. Additionally, Human Resource Management contracts with Kaiser Foundation Health Plan of the Mid-Atlantic States 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. As shown in Chart 1 below, premium revenue has exceeded claims expenses for each of the past two fiscal years, resulting in a cash balance of $350 million at June 30, 2018.

State Employee Health Insurance Fund
($ in millions)

Chart 1

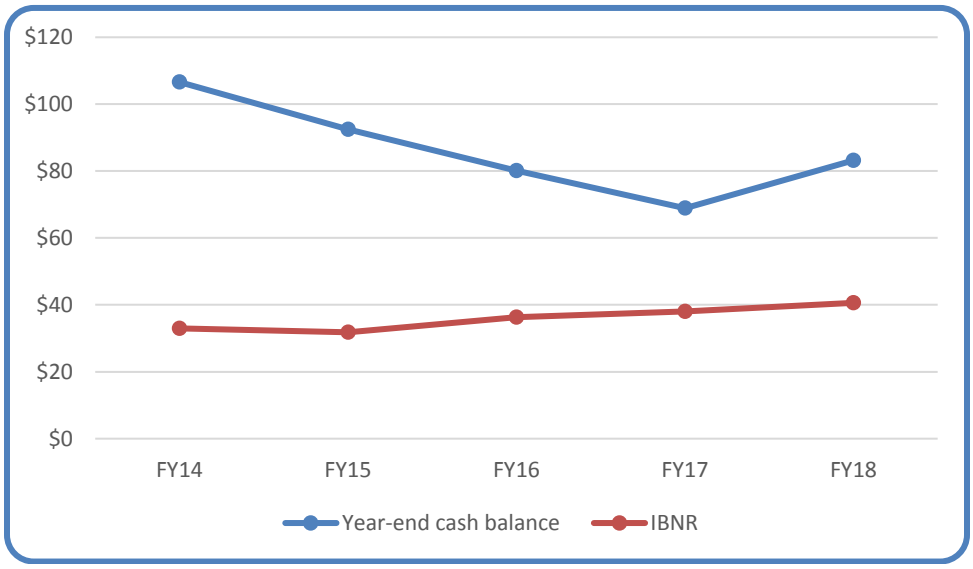


Local Choice Health Care Fund

Health Benefits Services administers the Local Choice (TLC) health benefits program, which provides health benefits and long-term care programs to local governments and school jurisdiction employees, dependents and retirees. Six health plans are available as options for the participating jurisdictions. Human Resource Management contracts with Anthem Blue Cross and Blue Shield and Kaiser Permanente to serve as the administrators of the TLC health plans. In fiscal year 2018, revenues exceeded expenses for the TLC fund for the first time since fiscal year 2014 as shown in Chart 2 below.

The Local Choice Health Care Fund
($ in millions)

Chart 2



Virginia Line of Duty Act Fund

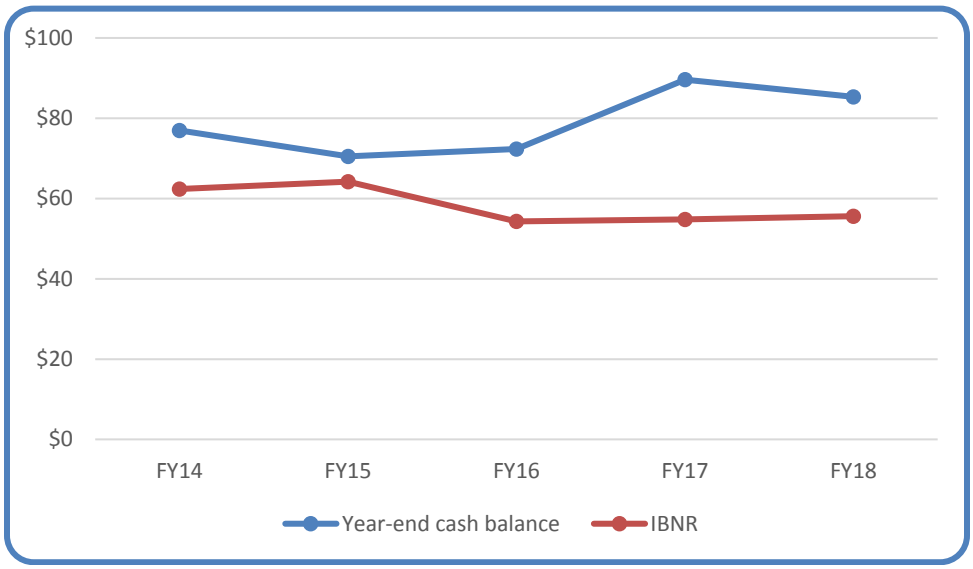
The Virginia Line of Duty Act (LODA), established under §9.1-400 of the Code of Virginia, provides benefits to eligible family members of eligible employees and volunteers killed in the line of duty, and to those eligible employees and volunteers disabled in the line of duty and their eligible family members. The Virginia Retirement System (VRS) is responsible for making all eligibility determinations and issuing benefit payments on behalf of entities that participate in the LODA Trust Fund administered by VRS. Beginning in fiscal year 2018, Human Resource Management is responsible for administering the LODA Health Benefits Plans. As of June 30, 2018, the cash balance in the LODA benefits fund is $4.6 million with an estimated IBNR of $2.7 million.

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. Human Resource Management contracts with Managed Care Innovations 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. Chart 3 below shows that cash balances have remained relatively consistent over the past five fiscal years.

Worker's Compensation Fund
($ in millions)

Chart 3



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 position, 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 state and local employees, employee dependents, and participating retirees.

Human Resource Management manages 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, and download reports to support absence management. Currently over 60 agencies with over 17,000 end users are using the system.

The Department of Accounts is in the process of developing an integrated component of the Commonwealth's accounting and financial reporting system, which will include functionality to replace Human Resource Management's personnel management; benefits management; and time, attendance, and leave systems. Representatives from Human Resource Management, with an expertise in human resources, benefits administration, and the current personnel management system, are working with the Commonwealth's accounting and financial reporting system team to aid in the project analysis phase, which is planned to continue through spring 2019.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 14, 2018

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Thomas K. Norment, Jr.
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, 2018. 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, 2018, which includes the Health Insurance Fund, the Local Choice Health Care Fund, the Line of Duty Act Fund, and the Worker's Compensation Fund. 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 management	Financial reporting
Revenues	Claims expenses
Actuary reporting	Service organization 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.

Our consideration of internal control was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and, therefore; material weaknesses and significant deficiencies may exist that were not identified. However, as described in the section titled "Audit Findings and Recommendations," we identified a deficiency in internal controls that we consider to be a material weakness and other deficiencies that we consider to be significant deficiencies in internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or

detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial information will not be prevented, or detected and corrected on a timely basis. We have explicitly identified one finding in the section titled "Audit Findings and Recommendations," to be a material weakness for the Commonwealth.

A significant deficiency is a deficiency or a combination of deficiencies in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We have explicitly identified five findings in the section titled "Audit Findings and Recommendations," as significant deficiencies for the Commonwealth.

As the findings noted above have been identified as material weaknesses or significant deficiencies for the Commonwealth, they will be reported as such in the "Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of the Financial Statements Performed in Accordance with Government Auditing Standards," included in the Commonwealth of Virginia Single Audit Report for the year ended 2018.

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.

Exit Conference and Report Distribution

We discussed this report with management on January 29, 2019. 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/vks

EMILY S. ELLIOTT
DIRECTOR

COMMONWEALTH of VIRGINIA

Department Of Human Resource Management

James Monroe Building
101 N. 14th Street, 12th Floor
Richmond, Virginia 23219
Tel: (804)225-2131
(TTY) 711

January 30, 2019

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

Dear Ms. Mavredes:

We have reviewed your report on the performance audit of the Department of Human Resources Management (DHRM) for the fiscal year ending June 30, 2018. We appreciate your staff providing a detailed review of each finding.

We acknowledge the weaknesses found in the preparation of information for financial disclosures under the Governmental Accounting Standards Board (GASB) Statement No. 75, related to postemployment benefits other than pensions. We are committed to and have already initiated corrective actions on the areas of noted concern. APA's recommendations were helpful in the building our plan forward and we have continued to work with staff at the Virginia Retirement System for further assistance when needed.

We acknowledge the deficiencies found in the areas of IT security governance, web application and security controls, and risk management and disaster recovery planning. We are committed to and have already initiated corrective actions on the areas of noted concern. We will continue to work with VITA through our agreement for Centralized ISO Services, as well as, take the necessary actions internal to the agency to address IT staffing concerns and priorities that must shift to focus on the corrective actions needed to avoid any further repeat findings. We do appreciate APA's recognition that some improvements were made during the audit period to address findings that were identified in prior audit reports.

Additional efforts are under way to address concerns noted with the review and documentation of service organization control reports of third-party service providers. Lastly, we have already implemented a process to ensure billing records are reconciled for the Line of Duty program.

I thank you and your staff for all of your assistance and guidance during our review.

Sincerely,

Emily S. Elliott
Director

An Equal Opportunity Employer

DEPARTMENT OF HUMAN RESOURCE MANAGEMENT

As of June 30, 2018

Rue Collins White, Acting Director

Richard Whitfield, Director
Contracts and Finance

Gene Raney, Director
Health Benefits Services

Kristie McClaren, Director
Workers' Compensation

Belchior Mira, Director
Information Technology