



SECRETARY OF FINANCE

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2014

Auditor of Public Accounts
Martha S. Mavredes, CPA

www.apa.virginia.gov

(804) 225-3350



AUDIT SUMMARY

This report summarizes our fiscal year 2014 audit results for the five agencies under the Secretary of Finance and arises from our work on the Comprehensive Annual Financial Report. Overall, our audit for the year ended June 30, 2014, found the following:

- Proper recording and reporting of transactions, in all material respects, in the Commonwealth Accounting and Reporting System and in the agencies' accounting systems;
- Internal control and compliance findings requiring management's attention; and
- Adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this report.

This report also includes information on the following significant initiatives and issues for agencies under the Secretary of Finance.

Status of System Development Project

The Commonwealth is in the process of implementing the Cardinal System, a statewide accounting and financial reporting system. The Commonwealth implemented Phase one of the Cardinal System project in December 2011 with the implementation of the Department of Transportation's financial system. Phase two of the implementation occurred in October of 2012 with the Department of Accounts implementing the base modules of Cardinal. Phase three, which involves an incremental rollout to all state agencies, will occur over the next two years with Cardinal becoming the official system of record by the end of fiscal year 2017.

The Commonwealth has developed a funding methodology to support system maintenance and operation costs for the Cardinal system. The funding model is an internal service fund model that relies on user charges based on rates that are approved by the Joint Legislative Audit and Review Commission.

Pension Accounting Changes

The Commonwealth will implement new Governmental Accounting Standards Board (GASB) standards which cover the accounting and reporting of pension activity by employers in fiscal year 2015. These standards increase the amount of pension liability and expenses the Commonwealth and its localities report in their financial statements.

Shared Responsibilities for Management of Retirement System Member Data

The Virginia Retirement System (the Retirement System) launched a web-based benefits management system that allows agencies to immediately access and update member and agency-

related retirement data. Each employer is now responsible for the reporting and reconciling of member data supporting retirement contributions. These changes increased the interdependency of key Commonwealth information systems supporting human resource and payroll activities.

Statewide Implementation of New Federal Grant Requirements

Effective December 2014, the Federal Government has approved new requirements which will impact multiple agencies in the Commonwealth who receive federal funds. Each federal granting agency implemented the Office of Management's and Budget's Uniform Guidance: *Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*. The new requirements are seen as the largest change in federal grants management in 30 years and this change will impact a wide array of activities.

The Commonwealth uses a decentralized approach to managing federal funds; therefore, the Department of Accounts (Accounts) will have a role in reviewing the new requirements and identifying responsible parties for compliance with the requirements. They anticipate completing this review no later than June 30, 2015.

–TABLE OF CONTENTS–

	<u>Pages</u>
AUDIT SUMMARY	
COMMENTS TO MANAGEMENT	1-13
<i>Status of System Development Project</i>	1-2
<i>Modernization of Financial Reporting Processes</i>	2
<i>Statewide Implementation of New Federal Grant Requirements</i>	3
<i>Pension Accounting Changes</i>	4-5
<i>Shared Responsibilities for Management of Retirement System Member Data</i>	5-13
INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS	14-25
FINANCE SECRETARIAT OVERVIEW	26-29
INDEPENDENT AUDITOR'S REPORT	30-34
APPENDIX A	35-39
AGENCY RESPONSES:	40-47
<i>Department of Accounts</i>	40-42
<i>Department of Planning and Budget</i>	43-45
<i>Department of Taxation</i>	46-47
AGENCY OFFICIALS	48

COMMENTS TO MANAGEMENT

Status of System Development Project

Applicable to: *Secretary of Finance, Secretary of Transportation, Department of Accounts, and Virginia Department of Transportation*

Cardinal System

The Commonwealth has continued to make progress on its Cardinal system implementation, which will replace the Commonwealth's financial system (CARS) with a modern, enterprise-wide financial system (base financial system).

This is a key project since the current accounting system is outdated both in terms of the technology and available functionality.

Cardinal's first implementation phase occurred in December 2011, with the implementation of the Virginia Department of Transportation's (Transportation) financial system. Phase two of the implementation occurred in October of 2012 with the Department of Accounts (Accounts) implementing the base modules of Cardinal. The base modules consist of general ledger, accounts payable, and a portion of the accounts receivable module. Phase three, which involves an incremental roll out of the base modules to all state agencies, will occur over the next two years with Cardinal becoming the official system of record for the Commonwealth beginning in fiscal year 2017. In October 2014, the first wave of phase three agencies began using Cardinal and these were primarily smaller agencies that key directly into Cardinal rather than into CARS. The remaining agencies that are part of phase three include those that have their own independent administrative systems that need to interface into Cardinal. These interfaces are complex to configure and require training and testing to ensure they work properly before these agencies go live to Cardinal starting in February 2016. Cardinal's base modules will provide the foundation for a modern financial system for the Commonwealth with the ability to add other modules and expand functionality in future projects.

The project development and implementation cost was \$58 million for phases one and two and was funded by Transportation and a working capital advance of approximately \$7.3 million. The project development and implementation budget is \$60 million for phase three and is funded by a working capital advance. Transportation funded all operating costs through fiscal year 2013. Charges to agencies in the form of an internal service fund rate will fund operating costs and repayment of the working capital advance starting in fiscal year 2014. A detailed description of the internal service fund rate is described on the following page in the section titled, "Enterprise Applications Internal Service Fund."

Enterprise Application Internal Service Fund

Item 260 of Chapter 806, 2013 Acts of Assembly, provides the authority for an internal service fund that Accounts will manage and authorizes the Secretary of Finance to establish a fee charged to agencies to support enterprise system administration.

The rate for the Cardinal system will be \$1.05 per transaction for agencies. Transportation is using additional modules not being used by any other agency and therefore will be charged a separate additional rate of 36.2 percent of budgeted annual operating costs of the system. The rate was collected through quarterly payments beginning in fiscal year 2014. Fiscal year 2015 and subsequent years' rates will be adjusted based on profit/loss in the fund. Rates will increase in fiscal year 2017 to account for the repayment of the working capital advance.

Accounts and Planning and Budget developed a funding methodology to support system maintenance and operation costs for the Cardinal system and in October 2012, the Joint Legislative Audit and Review Commission approved the rates.

Modernization of Financial Reporting Processes

Applicable to: Department of Accounts

While a modern financial system will provide some of the flexibility and technology needed, the Commonwealth is at risk of issuing inaccurate financial reports or not being able to comply with state or federal mandates for more comprehensive and timely reporting without changing its current financial reporting processes, particularly in light of the changing accounting and regulatory environment and reduced administrative personnel at the agency level. We recognize that it takes time to implement these changes and that Accounts has focused its efforts primarily on the development and implementation of the Cardinal System. As the Commonwealth moves closer towards implementing the Cardinal System at the statewide level, we continue to emphasize the importance of Accounts re-examining the Commonwealth's financial reporting process to identify opportunities for improving its use of technology, communication with agencies, and analysis of financial activity.

Statewide Implementation of New Federal Grant Requirements

Applicable to: *Department of Accounts, the Auditor of Public Accounts, and all agencies, which receive or have oversight of practices governing federal awards*

Final Interim Rule

On December 19, 2014 each federal granting agency issued an interim joint final rule to the Federal Register to implement the Office of Management and Budget's (OMB) Uniform Guidance: Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (Uniform Guidance). The Uniform Guidance replaces eight separate documents, known as Circulars, which were previously used to govern grants management. While some of the requirements from the Circulars were carried forward to the new Uniform Guidance, there are new requirements within the Uniform Guidance that the Commonwealth will need to comply with when it agrees to accept federal funds.

Implementation Schedule

The Uniform Guidance became effective on December 26, 2014. In practice, the Commonwealth is required to implement the final guidance when it receives a federal award with terms and conditions that incorporate the Uniform Guidance on or after December 26, 2014. This means that going forward each agency in the Commonwealth will need to review its federal awards to determine if they are required to follow the old Circulars or the new Uniform Guidance. Additionally, Commonwealth agencies that pass through federal funds to sub-recipients will need to communicate to their sub-recipients which federal funds require compliance with the new Uniform Guidance. However, the new audit requirements under the Uniform Guidance will apply across the board to the Commonwealth's fiscal year 2016 Single Audit.

Ensuring the Commonwealth's Compliance

The new Uniform Guidance is seen as the largest change in federal grants management in 30 years. It impacts a wide array of activities, including, but not limited to, time and effort practices, procurement policies, and Commonwealth-wide reporting of federal expenditures. As a result of the breadth of changes, multiple Commonwealth agencies will be required to change their policies and practices to ensure the Commonwealth is in compliance with the new requirements. The Commonwealth uses a decentralized approach to managing federal funds; therefore, the Department of Accounts (Accounts) plans to identify each of the individual requirements as either the responsibility of Accounts or another agency (ies). Accounts expects that they will, no later than June 30, 2015, communicate the results of its analysis to all agency fiscal officers, and, according to Accounts, each fiscal officer will be responsible for ensuring compliance with all applicable reporting requirements of the new Uniform Guidance.

Pension Accounting Changes

Governmental Accounting Standards Board (GASB) Statement No. 67, which covers accounting and reporting by pension plans, was implemented by the Virginia Retirement System in fiscal year 2014. This standard had minimal impact on the pension related information included in the Commonwealth's fiscal year 2014 financial statements. However, GASB Statement No. 68, which covers accounting and reporting of pension activity by employers and the Commonwealth and its various localities will implement in fiscal year 2015, will have significant impact on the Commonwealth's financial statements. Accounts and the Virginia Retirement System will work together to coordinate the Commonwealth's implementation of these new standards.

The new standards have a conceptual shift in the reporting of liabilities and expenses from a funding approach to an earnings approach. Currently, the Commonwealth only reports a liability to the extent it did not fully fund the annually required contribution as determined by its actuary. Under the new standards, the Commonwealth will report a pension liability as employees earn their benefits by providing services, which will result in a large increase in the Commonwealth's net pension liability and expense in its financial statements. The Commonwealth is allowed to offset the pension liability by the assets it has accumulated to fund the benefits to arrive at the net pension liability in its financial statements. These changes will result in the pension liability being reported in a similar manner as other long-term obligations by including them on the face of the financial statements and not just in the notes to the financial statements.

The Commonwealth's pension expense under Statement No. 68 will be based on the change in total pension liability from year to year. The Commonwealth will recognize some of the expense immediately and defer part of the expense to later years. Previously, the GASB expense, which is based on the annual required contribution, was also the standard for responsible funding. The Virginia Retirement System has recently adopted a new policy for funding pension plan costs, which is consistent with guidance developed by a national Pension Funding Task Force. This policy encompasses actuarial cost and asset smoothing methods and amortization policies that appropriately balances pension costs to the generation of taxpayers that received the services.

If the government has adopted a funding strategy to fully fund the net pension liability, they are allowed to continue to use the long term expected rate of return during the period that assets are accumulated to reach the fully funded status.

Current standards require a discount rate equal to the long-term expected rate of return on the pension plan's investments. Under the new standards, if the pension plan's investments are not sufficient to cover all of the projected benefit payments, the Virginia Retirement System will be required to use a blended rate consisting of the long-term expected rate of return and the municipal borrowing rate for the portion not covered.

Statement No. 68 will also require pension obligations and Required Supplementary Information (RSI), which are currently only reported in the Commonwealth's Comprehensive Annual

Financial Report, to now be reported in the financial statements of higher education institutions and certain agencies that produce their own financial statements, such as the State Lottery Department and Department of Alcoholic Beverage Control. The Virginia Retirement System will provide these entities with the liability amounts and RSI information for inclusion in their financial statements.

Finally, government employers participating in cost-sharing multiple-employer plans must recognize their proportionate share of the collective amounts for the plan as a whole. Currently, the main impact of this change will be an increase in the net pension liability reported in the financial statements of the Commonwealth's localities. The amount of the pension liability required to be reported by the localities could be reduced if the General Assembly passed legislation that modifies how the Commonwealth makes the payment for its portion of teachers' pension. The Virginia Retirement System has provided information to the localities estimating the extent of this increase and will annually provide the localities with liability amounts and other required information, which will be audited by the Auditor of Public Accounts so that it can be relied upon by the localities' auditors.

Under current statutes, the Commonwealth's localities will be required to report a large net pension liability in their individually published financial statements for teachers covered under the cost sharing multiple employer plan administered by the Virginia Retirement System.

Shared Responsibilities for Management of Retirement System Member Data

The Virginia Retirement System (the Retirement System) manages multiple pension plans and other post-employment benefits on behalf of its more than 800 participating employers. Member data supplied by the participating employers drives the calculation of retirement contributions as well as financial reporting for the Retirement System and the employers. Various information systems, supporting human resource and payroll activity at the employer level and operations at the Retirement System, store member data.

In fall 2012, the Retirement System launched *myVRS Navigator*, a web-based benefits management system that allows employers to immediately access and update member and agency related retirement data. The implementation of *myVRS Navigator* significantly changed the member data collection and retirement contribution reporting processes. With its implementation, many of the responsibilities for managing member data shifted from the Retirement System to each employer.

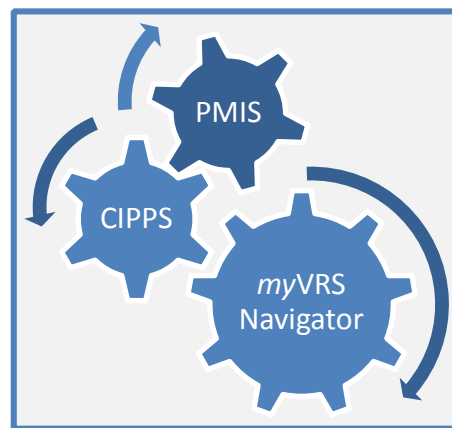
These changes have highlighted the interdependency of key Commonwealth information systems supporting human resource and payroll activities and the risks created when they are out of sync, while giving the agencies more automated tools to ensure their accuracy. The majority of state agencies use these systems, which are maintained by three central agencies: the Retirement System, the Department of Accounts (Accounts), and the Department of Human Resource Management (Human Resource Management).

This comment to management focuses on the responsibilities of these central agencies and those state agencies using these systems to manage member data. However, many of the issues surrounding the management of member data discussed below are relevant to other participating employers within the context of their operational environments. Therefore, all employers participating in plans administered by the Retirement System should consider the information presented here.

Commonwealth Systems are Now Interfaced to myVRS Navigator to Share Member Data

Under the new process, three Commonwealth information systems directly support member data and retirement contribution reporting:

- the Retirement System's *myVRS Navigator*,
- Human Resource Management's Personnel Management Information System (PMIS); and
- Account's Commonwealth Integrated Payroll and Personnel System (CIPPS).



All three systems now electronically share certain data elements with one another, which were previously independently keyed into the Retirement System's legacy system. These data elements support the calculation and payment of retirement contributions monthly; and serve as the foundation for the actuarially determined pension liabilities for the retirement plans managed by the Retirement System.

Specifically, PMIS interfaces daily with *myVRS Navigator* and CIPPS, passing on member data elements relevant to each system, such as position, hire date, salary, and birthdate. *myVRS Navigator* uses the data to apply service credit to member accounts and calculate the expected monthly retirement contributions for the individual member and the agency as a whole. *myVRS Navigator* generates a monthly billing file containing the calculated monthly retirement contribution data. CIPPS in turn generates a set of reconciliation reports for each agency based on the *myVRS Navigator* file and payroll calculations driven by the data interfaced from PMIS. Based on the resolution of these reconciliations, Accounts will make adjustment payments for instances where under or over payments have occurred.

Because of the direct linkage of critical fields between the three systems, each agency must ensure they enter all required fields in PMIS, so that the data pushed to the other systems is accurate. The importance of accurately capturing member data within PMIS has elevated the significance of PMIS in the day-to-day management of member data housed in *myVRS Navigator* as well as payroll

related data housed in CIPPS. It has also expanded the need for agencies' human resource staff to participate in the reconciliation process between the three systems.

Responsibility for the Accuracy of Employee/Member Data has Shifted

In the past, agencies submitted forms to the Retirement System who would in turn update the member data within the Retirement System's legacy system. With the interfacing of PMIS, myVRS Navigator, and CIPPS, the Retirement System no longer holds the source documentation for changes to agency and member data; and instead it resides with the agency. Therefore, to ensure the accuracy of member data and their retirement contributions, the agency must ensure the three systems remain in-sync, by promptly updating information, especially in PMIS, and thoroughly reconciling data between all three systems.

Commonwealth policies require each agency to confirm Retirement System contributions monthly through a "snapshot" of the agency's expected contribution in total and by member, based on the data in myVRS Navigator at the time of the "snapshot." This confirmation becomes the official basis for the billing of retirement contributions and the payable due from the agency.

As the three systems share the data elements that are the basis for the retirement contribution calculation, confirming the contribution "snapshot" without researching any existing variances can cause errors in members' retirement related data. It can also lead to an agency under or overpaying retirement contributions to the Retirement System creating complications when a member retires.

Importance of the Member Data to Individual Agencies is Changing

Further, in the past the actuarially determined liability resulting from an agency's participation in the retirement plans administered by the Retirement System, were reported in the footnotes of the Retirement System and Commonwealth's Comprehensive Annual Financial Reports. Beginning in fiscal year 2015, due to the implementation of Governmental Accounting Standards Board's (GASB) Statement No. 68 as discussed previously, that liability will be reported in the Commonwealth's basic financial statements, as well as in the financial statements of any individual agencies who issue them.

Beginning in fiscal year 2015, pension liabilities will be reported in the Commonwealth's basic financial statements as well as in the financial statements of any individual agency who issues them.

Our work at the agency level for fiscal year 2014 did not indicate any materially significant discrepancies that would affect the accuracy of the actuarially determined liability. We did not audit every agency; however, for the agencies we audited, we did observe some issues with:

- the timeliness and thoroughness of investigation by the agencies of errors identified by the reconciliations between the three systems,
- the timeliness of the “snapshot” confirmation,
- the accuracy of member data between the three systems, and
- in a few minor instances, the accuracy of the member data itself.

These observations could place the Retirement System, the Commonwealth, and its agencies at risk from a financial reporting perspective, if observed more frequently. It is imperative that each agency understand the importance of reconciling and confirming retirement contributions and promptly addressing exceptions between the member data stored in PMIS, *myVRS* Navigator, and CIPPS.

Guidance, Training and Tools Exist, but are Being Enhanced

Since 2012, the Retirement System and Accounts together have published guidance in their respective regular employer communications, offered training, and conducted outreach to state agencies to guide them in the data entry, reconciliation, and contribution confirmation processes. Depending on the activity, agencies have different resources available to them as reflected on the following page.

Navigation and Data Entry for myVRS Navigator	•VRS Employer Manual http://www.varetire.org/employers/manual/index.asp •myVRS Publications http://www.varetire.org/publications/index.asp?ftype=myvrs •Frequently Asked Questions about myVRS Navigator http://www.varetire.org/pdf/publications/vnav-faqs.pdf •TRAINING: VRS University Online Courses http://www.varetire.org/employers/training/vrs-university.asp
Benefits Processing and Reconciliation	•VRS Employer Updates http://www.varetire.org/employers/update/index.asp •DOA Payroll Bulletins http://www.doa.virginia.gov/Payroll/Payroll_Bulletins/Payroll_Bulletins_Main.cfm •TRAINING: DOA Payroll Operations http://www.doa.virginia.gov/Payroll/Training/CIPPS_Intro_Training/CIPPS_Training_Manual.cfm •TRAINING: VRS University Online Courses http://www.varetire.org/employers/training/vrs-university.asp
Daily and Monthly Reconciliation Tools	•Benefits Processing Reports Appendix http://www.doa.virginia.gov/Payroll/Training/CIPPS_Intro_Training/CIPPS_Training_Manual.cfm •Calculation Spreadsheets: VRS Automated Recon Spreadsheet http://www.doa.virginia.gov/Payroll/Forms/Payroll_Forms_Main.cfm •PMIS to CIPPS Update Crosswalk http://www.doa.virginia.gov/Payroll/Forms/Payroll_Forms_Main.cfm
Agency Specific Processing Questions	•VRS Employer Support Team http://www.varetire.org/employers/support/employer-support-team.asp •DOA Payroll Operations http://www.doa.virginia.gov/Payroll/Payroll_Main.cfm

Accounts’ periodic “Payroll Bulletin” and the Retirement System’s monthly “Employer Update” currently provide the best guidance for ensuring the member data remains in-sync between the three systems; and that the reconciliations and confirmations are performed properly. While the guidance exists, because it is separated into different publications, it is more challenging for employers to locate and follow.

The Retirement System is in the process of publishing additional sections to its employer manual that will consolidate the guidance provided in their Employer Updates into one document. They expect to finalize their updates by the end of January 2015. Likewise Accounts is working towards consolidating their guidance in to the Commonwealth Policies and Procedures (CAPP) Manual, which they anticipate completing by the end of March 2015. The Retirement System and Accounts should give priority to this activity to ensure the guidance provided remains current, consistent and easily accessible. Accounts should also ensure they clarify the responsibilities of

agencies using the Payroll Service Bureau or other payroll services within Accounts, as there are different expectations for these entities.

In the interim, several educational avenues exist. Through the VRS University Online Course system, the Retirement System provides web based training courses supporting *myVRS* Navigator and the Contribution Confirmation process, most specifically the course on “Contribution Confirmation and Payment Scheduling.” This course addresses the following relevant topics: Create Snapshot, Review Snapshot, Reconcile Snapshot, and Confirm Snapshot, and is available for all participating employers. Additionally Accounts offered joint in-person training session with the Retirement System for agency human resource and payroll staff. Accounts is uncertain when they will offer this in person training again; however, the slides are available on Accounts’ website, as referenced above. While not currently scheduled, Accounts and the Retirement System should offer similar sessions in the future for new human resource and payroll staff at the user agencies.

Finally, Accounts, Human Resource Management and the Retirement System have recently initiated monthly status meetings with each other. These meetings are designed to ensure Accounts, Human Resource Management, and the Retirement System remain aware of existing and emerging agency concerns regarding these processes. Through the meetings Accounts, Human Resource Management and the Retirement System plan to expand and enhance the guidance and tools cited above to better support the efficient and effective execution of these processes. We encourage the continued use of this meeting venue to ensure communications with agencies remain consistent and cohesive regarding the processes and tools available. In addition, Human Resource Management should consider how their communications with human resource staff at the individual agencies and training can be expanded to highlight the importance of their role in these processes.

Prioritization Should Be Given to Accurately Manage Member Data by all Agencies

While the new data interfaces and reconciliations developed by Accounts, Human Resource Management, and the Retirement System provide tools to more efficiently manage member data, they have also highlighted the interdependency of the member data maintained in CIPPS, PMIS, and *myVRS* Navigator and the risks created when they are out of sync. Most notably, the relevance of PMIS in relation to the processing of payroll and retirement contributions has grown tremendously, changing the focus of timing for data entry into this system.

The new processes require ongoing coordination and communication between each agency’s human resource department and the corresponding payroll department. Each agency must ensure their respective departments sufficiently prioritize maintaining the accuracy and integrity of member data. By doing so in the long term, agencies should realize many efficiencies in the management of member data. However, the path to realize those efficiencies may take time until the new processes are fully adopted within each agency and the reconciliation exceptions which have developed over time are fully addressed.

For example, prior to the implementation of *myVRS Navigator*, the Retirement System directly keyed data into their legacy system. Only a few key fields had to be entered in PMIS timely to support payroll processing, the remaining fields could wait. With the implementation of *myVRS Navigator*, PMIS now serves as the initial system of record for numerous critical data elements electronically transferred to CIPPS and *myVRS Navigator*. As a result, each human resource department must ensure they promptly enter all of the required data elements into PMIS to support accurate and timely retirement contributions and payroll processing.

To help agencies ensure the integrity and accuracy of member data, Human Resource Management should develop reports or better highlight the availability of existing reports which identify key data fields missing in PMIS. By ensuring the initial system of record for the member data is accurate, and updated promptly with changes, many of the reconciliation exceptions currently being identified between the three systems could be eliminated.

Each agency must ensure they have adequate policies and procedures developed to support the investigation of interfacing errors between the three systems and the confirmation of the monthly “snapshot.”

Further, each agency must ensure they have adequate policies and procedures developed to support the investigation of interface errors between the three systems, as well as the confirmation of the monthly “snapshot.” While Accounts and the Retirement System have developed specific reconciliation reports and tools to support these processes, the unique nature of each agency in size and structure prohibits them from developing a singular approach for executing them.

Each agency needs to consider the expectations laid out in the guidance provided by Accounts and the Retirement System and ensure they have sufficient policies and procedures in place to meet these expectations. Most importantly, agencies must ensure they promptly address the reconciliation of exceptions between *myVRS Navigator* and PMIS, *myVRS Navigator* and CIPPS, and PMIS and CIPPS. Doing so will help to ensure the contribution calculations, payroll withholdings, and contribution payments are accurate.

Monthly Reporting Deadlines Should be Enforced

To emphasize the importance of all of these processes, the Retirement System should begin enforcing the monthly deadline for the retirement contribution “snapshot” certification. The Retirement System will only send the monthly billing file to Accounts after all of the CIPPS user agencies certify their monthly “snapshot.” Enforcing the deadline will allow Accounts to complete the necessary steps to ensure timely and accurate adjustments to payments of retirement contributions previously submitted on behalf of the CIPPS user agencies. By completing the pre-certification reconciliations with the PMIS systems, and timely certification of the “snapshot”, individual agencies will reduce the number of reconciliation exceptions to be resolved decreasing their administrative efforts and improving data accuracy. Likewise, the Retirement System will realize even greater accuracy and integrity of the data supporting contribution reporting and actuarial calculations.

All Participating Employers Should Remain Diligent in Managing Member Data

This comment to management focuses specifically on state agencies who use PMIS and CIPPS to manage their human resource and payroll functions. However, given the ramifications of GASB Statement No. 68, all employers participating in the plans administered the Retirement System should remain cognizant of their role in ensuring the accuracy of member data and retirement contributions submitted to the Retirement System. The Retirement System, likewise, should ensure they continue to provide sufficient guidance and enforce reporting expectations for these employers.

As reflected above, for the Commonwealth, the efficient and effective management of member data requires the coordinated effort of all three central agencies as well as individual agencies on an ongoing basis. This comment to management highlights the importance of these efforts and the impact they have on each organization. To ensure each organization appreciates the risk and focuses the appropriate resources on the management of member data, we summarize below their respective responsibilities moving forward.

Key Actions for Maintaining and Reporting Member Data Moving Forward

Individual Agencies

- Developing internal policies and procedures to promptly execute the data entry, reconciliation and certification processes in accordance with central agency guidance within the constraints of their organization.
- For agencies using a payroll service provider, clarifying the roles and responsibilities of the agency and the service provider.
- Ensuring all critical fields are promptly updated in PMIS.
- Ensuring human resource and payroll departments are fully engaged in supporting these processes and adequately communicate with each other.

Virginia Retirement System

- Focusing on completing the update of the Employer Manual to consolidate all issued guidance regarding the reconciliation of member data and validation of retirement contributions.
- Enhancing existing and developing new tools, reports, and training to support agency and other employers needs, coordinating with Accounts and Human Resource Management as needed.
- Enforcing monthly reporting deadlines.

Department of Accounts

- Focusing on updating the CAPP Manual to consolidate all issued guidance regarding the reconciliation of member data and validation of retirement contributions.
- Enhancing existing and developing new tools, reports, and training to support agency needs, coordinating with Human Resource Management and the Retirement System as needed.
- For agencies using the Payroll Service Bureau or other payroll services within Accounts, clarifying the roles and responsibilities of the service provider and the agency.

Department of Human Resource Management

- Enhancing existing and developing new tools, reports, and training to support agency needs, coordinating with Accounts and the Retirement System as needed.
- Expanding communications with human resource staff to highlight their roles and responsibilities in the successful management of the Retirement System's member data through PMIS.

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Controls over Cardinal Security

Applicable To: Department of Accounts

The Department of Accounts Cardinal Team is not properly managing access to the Cardinal system. During our review, we noted the following:

- Sixty-one employees with access to Cardinal who did not log on during the entire fiscal year 2014, indicating they are dormant users and potentially no longer require access.
- Several instances of self-approved journal entries, indicating that users have access to both enter and approve the same transactions.

The Commonwealth's Information Security Standard SEC501-08, (Security Standard), AC-2-COV, Part B, instructs all agencies: "For all internal and external IT systems, disable unneeded accounts in a timely manner." Also, having dormant accounts for an extended period of time goes against industry best practices. Further, instances of self-approved transactions represent violations of proper separation of duties.

The Cardinal Team has a process for regularly monitoring system access; however, this process does not include a review of dormant accounts. Not removing access on dormant accounts increases the risk of unauthorized transactions and could impact the integrity of the Commonwealth's financial systems.

The Cardinal Team allows users to both enter and approve journal entries because some individuals are serving dual roles as backups for other individuals. Transactions that are entered and approved by the same individual are reviewed periodically; however, since this may be well after the transaction has occurred, there is still the risk that improper transactions can occur. Although a physical approval may take place outside the system for these transactions, this does not initially ensure proper entry into the accounting system.

The Cardinal Team should enhance their management of access by regularly reviewing and removing access for dormant accounts. In addition, the Cardinal Team should consider removing the ability for users to both enter and approve journal entries, as generally a preventative control is more effective than the current detective control.

Improve Payline Web Application and SQL Server Database Security

Applicable To: Department of Accounts

The Department of Accounts (Accounts) does not secure the Payline web application and supporting database with the minimum security controls required by the Security Standard. Payline is a web-based system that reports the earnings statements for all state employees and contains personally identifiable information. We identified six control weaknesses which we 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. The Security Standard requires implementing specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability.

We recommend that Accounts dedicate the necessary resources to implement timely the controls discussed in the communication marked FOIA-Exempt in accordance with the Commonwealth's Security Standard.

Improve Risk Management and Continuity Planning Documentation

Applicable To: Department of Accounts

Accounts does not have up-to-date risk management and continuity planning documentation, which includes the Business Impact Analysis (BIA), Risk Assessments for sensitive systems (RA), Continuity of Operations Plan (COOP), and Disaster Recovery Plan (DRP). Accounts has not updated its BIA or RAs since 2010 and has not updated the COOP and DRP since April of 2011 to reflect its current environment.

The Security Standard, Section 3, requires agencies to conduct periodic reviews and revisions of the agency BIA, as needed, but at least once every three years. The Security Standard requires agencies to update its RAs of all IT systems classified as sensitive as needed, but not less than once every three years. Agencies must also conduct an annual self-assessment to determine the continued validity of the RA. Furthermore, the Security Standard requires the COOP and DRP to be based on the results of the BIA and RA, and requires agencies to conduct at least an annual exercise of the DRP to assess its adequacy and effectiveness. Lastly, the Security Standard requires the organization to update the contingency plan to reflect any material changes to the organization, information systems, operating environment, and problems encountered during contingency plan implementation, execution, or testing.

Accounts did not perform the necessary reviews and revisions to the Risk Management and COOP documentation due to a lack of resources. Therefore, Accounts is increasing the risk of not being able to restore essential business functions and supporting resources in the event a disaster occurs and during the performance of necessary restoration efforts.

We recommend that Accounts dedicate the necessary resources to revise, approve, and test the Risk Management and COOP documentation, following the requirements of the Security Standard.

Improve IT Security Audit Plan

Applicable To: Department of Accounts

Accounts does not have an updated IT Security Audit Plan. Additionally, Accounts' IT Security Audit Plan is not consistent with its BIA and system RA documentation. Further, Accounts has not performed IT security audits over all systems classified as sensitive once every three years, nor submitted an IT Security Audit Plan to the Commonwealth's Chief Information Security Officer (CISO) on an annual basis.

The Commonwealth's IT Security Audit Standard, SEC 502-02, Sections 1.4 and 2.1 (IT Audit Standard), requires that agencies develop and maintain an IT security audit plan for the IT systems for which it is the Data Owner. The IT Audit Standard requires agencies to base its IT security audit plans on the BIA and the systems data classifications and submit the updated plans to the Commonwealth's CISO on an annual basis. Lastly, the IT Audit Standard requires IT systems that contain sensitive data to be assessed at least once every three years in accordance with requirements of the Security Standard.

Accounts is increasing the risk that system vulnerabilities and threats remain undetected and are not reasonably secured in accordance with the Security Standard by not having periodic IT Security Audits performed on sensitive systems. Further, Accounts is not maintaining an up-to-date or complete sensitive systems inventory nor updating BIA and risk management documentation to ensure consistency with the currently developed IT Security Audit Plan. Lastly, Accounts did not file an IT Security Audit Plan with the Commonwealth's CISO on an annual basis due to lack of resources.

We recommend that Accounts dedicate the necessary resources to create an up-to-date sensitive systems inventory and use that inventory to create an IT Security Audit Plan based on the requirements in the Security and IT Audit Standards. Accounts should update its BIA and risk management documentation, which will assist in maintaining a current and effective IT Security Audit Plan. Furthermore, Accounts should submit the necessary documentation to the Commonwealth's CISO on an annual basis as required by the IT Audit Standard.

Improve Internal Controls over System Access

Applicable To: Department of Planning and Budget

The Department of Planning and Budget (Planning and Budget) does not have adequate policies and procedures for granting and deleting agency user access in the Performance Budgeting (PB) system. Additionally, Planning and Budget does not provide detailed guidance to agency

administrators on the specific capabilities of user roles within the PB system. Planning and Budget's lack of adequate access controls over the PB system increases the risk of agency employees with inappropriate access.

Section 8.1 of the Security Standard requires formal, documented policies and procedures to implement account management practices for requesting, granting, administering, and terminating user accounts. Further, that section of the standard requires the granting of users' access on the principle of least privilege.

Planning and Budget currently has an informal process of granting and deleting user access in the PB system, which consists of email correspondence between Planning and Budget and the requesting agency. Planning and Budget has not established specific policies to direct how the process should work. Additionally, agency administrators, who maintain the authority to determine who and what level of access their employees can obtain, have not been provided up-to-date PB system policies that clearly delineate user capabilities at the user role level, which are module specific. Planning and Budget has not provided sufficient guidance to allow agency administrators to determine if permission is being granted based on what's minimally required to accomplish assigned tasks.

To decrease the risk of inappropriate PB system access and enhance overall system access controls, we recommend that Planning and Budget develop and adhere to policies for granting and disabling PB system user access. While we recognize that PB system transactions do not have an immediate impact on financial information as recorded in the Commonwealth's accounting system, based on the required levels of approval, system owners still have minimal requirements to which they should adhere as outlined in the Security Standard. Planning and Budget should provide reference material that includes descriptions of user role capabilities within each module to all agency administrators to ensure access is being granted based on the principle of least privilege at the agency level.

Enhance Performance Budgeting System Access Reviews

Applicable To: Department of Planning and Budget

Planning and Budget does not consistently perform, track or complete adequate follow-up of periodic PB system access reviews to ensure that agency access permissions remain appropriate over time as employees change positions and responsibilities at the agency level. Additionally, Planning and Budget does not have formal, documented policies that require or describe the procedures that take place during the system access review process. Planning and Budget's lack of adequate access controls over the PB system increases the risk of agency employees with inappropriate access.

Section 8.3 of the Security Standard requires agencies to develop, disseminate, and review system access at least annually. The Standard also requires formal, documented procedures to

facilitate the implementation of the review. Further, the Security Standard requires reviews of information systems be tracked to accurately demonstrate account creation, disabling and termination actions taken. Planning and Budget's lack of adherence to the applicable portions of the Security Standard for system owners increases the risk of agency employees with inappropriate access.

Currently, Planning and Budget performs an annual review of PB system access, which involves contacting agency administrators and requesting that agency administrators review users as listed in the PB system. Planning and Budget requests that administrators only respond if the administrator identifies accounts that should be disabled but does not require administrators to review access to ensure access privileges held are still reasonable for employees' based on their current job responsibilities, nor does it require administrators to certify the reasonableness of agency access if there are no changes that need to be made. For agencies that respond to Planning and Budget with accounts to disable, Planning and Budget maintains the email signifying that an agency requested an access change. Planning and Budget's current process does not incorporate a mechanism for determining that all changes requested by the agencies are actually performed in a timely manner.

While we recognize that PB system transactions do not have an immediate impact on financial information as recorded in the Commonwealth's accounting system, based on the required levels of approval, system owners still have minimal requirements to which they should adhere as outlined in the Security Standard. We recommend that Planning and Budget develop and adhere to policies surrounding its annual review of PB system access at the agency level. The policies at a minimum should require agencies to provide positive confirmation that all access levels held by agency employees are reasonable and necessary for the employee to perform current job responsibilities. Planning and Budget should also assess the number of agency administrators assigned to each agency to determine if it is reasonable based on the size and nature of the agency. Lastly, Planning and Budget should ensure its review process is accurately tracked, to easily identify unresponsive agencies and to demonstrate that its review process is complete and being performed in a timely manner.

Improve IT Risk Management and Disaster Recovery Planning Programs

Applicable To: Department of Planning and Budget

Planning and Budget does not consistently define or perform essential elements of its Risk Management and Disaster Recovery Planning programs. These processes are essential for an organization to assess and mitigate systems security risks and threats to business operations and supporting information systems.

Section 8 of the Security Standard requires the identification of system vulnerabilities, threats, safeguards, threat probabilities and loss impacts. Further, the Security Standard requires individual risk assessments for all sensitive systems identified in an agency's Business Impact Analysis

and requires an annual self-assessment of its sensitive system risk assessments. Lastly, the Security Standard requires agencies to perform annual exercises to assess the adequacy and effectiveness of its Disaster Recovery Plan (Plan).

Planning and Budget's current risk assessment, which includes three mission essential systems, does not maintain all requirements of the Security Standard. Additionally, Planning and Budget does not have individual risk assessments completed for all sensitive systems as outlined in its Business Impact Analysis. Lastly, Planning and Budget is not conducting annual self-assessments of its sensitive systems nor performing annual exercises to assess the effectiveness of its Plan.

Planning and Budget's lack of completed risk assessments across all sensitive systems increases the risk that any known system threats and vulnerabilities will not be appropriately considered, planned for, or mitigated. The lack of a performed exercise of the Plan increases the risk that in the event of a disaster, Planning and Budget will not be able to effectively recover from system backups, or prioritize the order in which to restore systems. Further, Planning and Budget's failure to exercise its Plan on a regular basis could ultimately lead to significantly affected or compromised business operations.

These weaknesses are primarily due to Planning and Budget's lack of available resources and staffing to reasonably develop and implement an adequate Risk Management and Disaster Recovery Program that meets the requirements outlined in the Security Standard. The role of the Information Security Officer is currently assigned as an alternate function of one Planning and Budget employee, and not having a dedicated security resource has resulted in the identified weaknesses in Planning and Budget's Risk Management and Disaster Recovery Programs.

We recommend that Planning and Budget dedicate the necessary resources to develop and implement an adequate Risk Management and Disaster Recovery Program. Planning and Budget should also dedicate the necessary resources to ensure the performance of Risk Assessments for all sensitive systems, as well as develop a processes to conduct annual self-assessments. Further, Planning and Budget should review the IT Risk Management requirements established in Section 8 of the Security Standard to ensure that their IT systems and data are appropriately classified. Lastly, we recommend that Planning and Budget annually test its Disaster Recovery Plan and reassess and improve the Plan based on the results of the tests.

[Improve Internal Controls over Advantage Revenue Access](#) (Partial Repeat Finding)

Applicable to: Department of Taxation

Taxation needs to strengthen its internal controls over systems access to ensure compliance with the Commonwealth's information security requirements. We continue to identify areas where system access controls need to be improved, including the general understanding and

documentation that explains Taxation's access structure and controls, granting of system access, and the annual recertification process.

The Security Standard addresses requirements over information system access controls. Section 8.1 AC-5 of the Security Standard addresses access controls and requires the organization to segregate duties of individuals as necessary, to prevent unauthorized activity. Further, Section AC-6 goes on to address the concept of least privilege and requires that an organization use the concept of least privilege when granting access to ensure users only have access which is necessary to accomplish its assigned tasks.

During our audit, we found instances where Taxation granted system access which was not in compliance with these requirements and these are detailed below. Taxation has a complex access structure and we believe these instances are occurring, at least in part, because Taxation is granting access in some instances without a clear understanding of the way the different components of the access structure work together to control access for an individual employee.

Taxation has a number of internal controls in place that compensate for the weaknesses in the access controls and to help to ensure that unauthorized transactions are not processed. We did not find instances where the weaknesses in access controls resulted in unauthorized transactions; however, failure to address these system access issues will continue to expose Taxation's information systems to unnecessary risk and result in noncompliance with information security requirements.

Taxation's System Access Structure

Taxation's access structure for the Advantage Revenue (AR) system, its critical financial reporting system, is granted through a combination of resources groups, access levels, security groups, and workgroups. In order to evaluate access for an individual employee, it is necessary to consider the relationship between each of these components and how this affects the functions available to the employee. Taxation also has established several special workgroups, commonly referred to as supervisor accounts, which enable a user to access transactions assigned to another user. These supervisor accounts were originally designed to facilitate backups in the event of an employee's absence.

Although Taxation has developed additional documentation on its access structure since our last audit, it remains very difficult to understand the relationships between the various components to fully understand and evaluate the access an individual employee has been granted. The difficulty is due to a lack of documentation as well as a lack of a system-wide understanding. Currently, employees who manage security group and workgroup access report to two different supervisors. This organizational structure, in combination with a lack of adequate documentation, makes it difficult for each area to fully understand how different components of the access structure work together when access is granted for an individual employee. As result, we believe these issues are a significant factor in the instances of the inappropriate systems access discussed in this finding.

SAFE and the Recertification Process

Taxation uses the System Access for Employees (SAFE) tool to document, monitor, and track all types of user access from physical building access to information systems access. While SAFE is Taxation's system for managing employee access, we have some concerns about the completeness and accuracy of the information in SAFE.

We reviewed information from SAFE in conjunction with system access tables to gain an understanding of and review employee access capabilities for AR. We found instances where certain types of access were not recorded in SAFE, as well as instances where the information in SAFE was not accurate. Taxation does not reconcile the information in SAFE to the actual AR access in the access tables; therefore, information in SAFE may not be an accurate representation of the system access and discrepancies between actual access and documented access will not be identified.

We selected a sample of users with access to REV1, a workgroup which controls journal vouchers pending approval. REV1 access was not documented in SAFE for 10 of the 21 (48 percent) users. In addition, we found that SAFE does not include employee access to supervisor accounts. As a result, for 15 of 22 (68 percent) users selected, the employee's manager was not aware the user had access to some of the supervisor accounts.

The lack of accurate information in SAFE impacts the effectiveness of Taxation's annual recertification process. Section AC-2 of the Security Standard requires that agencies perform an annual recertification of system access. During the recertification, Taxation managers review system access information in SAFE to ensure that users have appropriate access granted on the principle of least privilege. The lack of accurate information in SAFE can prevent managers from identifying and correcting instances of inappropriate access during the annual recertification process or other periodic reviews.

We reported on additional concerns with the annual recertification review in our previous audit. Last year, we found situations where managers recertified inappropriate access for their employees. To address this, Taxation provided additional information on security groups and workgroups to managers during the most recent recertification review in October 2014. We reviewed the information and found that while Taxation provided additional information to help managers better understand the process, this information was not presented in a manner that would give the managers a complete understanding of what functions their employees are capable of performing. As a result, it is questionable how effective the additional guidance was in improving the recertification process.

Segregation of Duties and Access Issues

Section AC-5 of the Security Standard requires agencies to enforce segregation of duties through authorized systems access. The current access structure combines some related resources or functions together in resource groups that are assigned to each security group. In some cases, this is creating a lack of segregation of duties issue. One resource group in particular, 'REVACCT', contains 'JVCREATE' and 'JVAPPROV', which allows the user to both create and approve journal vouchers.

We reviewed access for a sample 64 employees with critical access, and found that 25 of the 64 (39 percent) had access to the REVACCT resource group and the REV1 workgroup. This level of access gives an individual the ability to create, edit, and approve journal vouchers, creating a segregation of duties issue. Of the 25 users with this access, 9 users were directly granted this access while 16 users have this access through supervisor accounts which we discussed earlier. Although this access combination creates a segregation of duties issue, Taxation has a compensating control in place to prevent a user from approving a journal voucher that they created. This control, however, does not prevent a user from editing and approving a journal voucher without a secondary approval. We reviewed all journal vouchers approved during the fiscal year and found that 12 were adjusted and approved by the same employee. While the total amount of these adjustments was not material to the agency as a whole, this access combination creates a segregation of duties issue over journal voucher processing and increases the risk of unauthorized transactions.

We also found two users in Taxation's General Legal and Technical Services section with inappropriate access based on their job responsibilities. Both users were able to create abatements and discharges, which can be used reduce a taxpayer's tax liability, and one of the users could also update taxpayer bank account information. One of these instances occurred because the employee transferred from a different section and system access was not properly re-evaluated. Neither instance was identified or corrected as part of the recertification process which reinforces our earlier discussion on the ineffectiveness of the recertification process.

Recommendations

We recommend that Taxation strengthen its controls over systems access and ensure that its access structure appropriately enforces segregation of duties to minimize risk and ensure compliance with the Security Standard. We recommend that Taxation complete a reconciliation of critical AR access information in SAFE to the appropriate access tables to ensure the information in SAFE is accurate and complete. As part of this reconciliation, Taxation should ensure that all access granted is documented in SAFE and all access in SAFE has been granted. This will help ensure the accuracy of the information in SAFE going forward.

To further increase the effectiveness of the recertification process, Taxation should continue to help managers understand the access they are recertifying. By illustrating how the additional information should be used as managers review access in the recertification instructions, Taxation will be setting the expectation that the managers should reference the additional information provided as they consider the access they are approving. We also recommend the Office of Technology collaborate with managers from across the agency as they refine the additional information provided to managers to create a more user-friendly and understandable reference tool for the managers.

Additionally, Taxation needs to review system access, especially for critical AR functions, to ensure adherence to the concept of least privilege. As part of the review, Taxation should determine which levels of access create significant segregation of duty conflicts. These conflicts need to be identified so that these can be considered when system access is initially granted and as part of the annual recertification process. This is an important step to ensure compliance with the Security Standard and minimize risk from unnecessary system access.

It is our understanding that Taxation has begun the process of identifying and purchasing a replacement for SAFE. As part of this process, Taxation should take this opportunity to address the issues discussed in this finding.

Update IT Risk Management Plans

Applicable to: Department of Taxation

Taxation does not update its IT risk management plans in a timely manner. Taxation's IT environment is constantly changing and conducting periodic and timely threat and vulnerability evaluations are critical to establish proper safeguards for sensitive data.

The Security Standard and Taxation's internal policy requires timely updates to IT risk management plans, such as business impact analysis and risk assessments. Specifically, we found that Taxation does not meet the Security Standard's requirements in the following areas.

- Taxation does not have updated risk assessments that comply with its new risk management plan and the Security Standard. Taxation has not created system specific risk assessments since 2009. Additionally, the Risk Assessments from 2009 do not have all the elements required by the Security Standard. The Security Standard, Section RA-1, requires agencies to maintain updated IT Risk Assessments that are consistent with its risk management and contingency plans for all sensitive applications and systems as needed, but no later than once every three (3) years.
- Taxation does not have an updated business impact analysis (BIA) that meets the requirements established in Taxation's information security policy. Taxation has stated

that its BIA is currently out of date and needs to be updated in order to perform further risk assessments over its sensitive systems. Additionally, the outdated BIA does not include an adequate revision history to track changes and updates. Taxation's Information Security Policy, version 3, section "Required Security Reviews, Audits and Evaluations," requires annual reviews and revisions of the BIA. However, Taxation could not provide documentation that these annual reviews and revisions have occurred. Additionally, the Security Standard, Section 3.1, requires that agencies review and revise its business impact analysis as needed, but no later than once every three (3) years.

Taxation was unable to meet these security requirements due to a lack of dedicated IT security resources. Additionally, Taxation went through a recent transition to a new Information Security Officer. During this transition, information about the revision history for the BIA was lost. Taxation is in the process of interviewing and hiring a Risk Manager who will update these risk management and contingency planning documents and ensure that they meet the requirements defined in the Security Standard.

Without updated risk assessments and a business impact analysis, Taxation cannot accurately determine the appropriate information security safeguards to protect sensitive data. We recommend that Taxation dedicate the necessary resources to update and improve the risk assessment and business impact analysis component of its IT risk management plan to align it with internal policy and requirements in the Security Standard.

Improve Physical Security to Server Rooms

Applicable to: Department of Taxation

Taxation does not have appropriate physical security controls in place to protect IT systems that store sensitive taxpayer information. While these server rooms do not house servers with key financial information, failure to implement the requirements in the Security Standard may result in Taxation being unable to adequately protect sensitive IT systems from human risk, which may result in the compromise of sensitive Taxpayer information. During our review, we noted the following weaknesses:

- There are multiple Taxation employees who have access to the server rooms that do not have a documented job responsibility that requires server room access. As a result, Taxation is not implementing the principle of least privilege over server room access. Specifically, we found that 21 Taxation employees have access to the server rooms without a documented job responsibility that require physical access to the server room. The Security Standard, Section AC-6, requires that an agency allow employees access only when that access is necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

- Taxation does not require that all employees with physical access to the server rooms go through its formal authorization process. Seven percent of Taxation's employees who have badge access to the server rooms without formal authorization documentation. The Security Standard, Section PE-3, requires that an agency enforce physical access authorizations for access to facilities where information systems reside.
- Taxation has not assigned the responsibility of reviewing physical access to sensitive IT systems that contain taxpayer information to an employee who does not have access to the same systems. Taxation should use appropriate separation of duties to ensure that the person that is responsible to review daily activity logs does not also have access to the server room. Additionally, the employee responsible for reviewing daily activity should be informed about the job responsibilities of each employee who has access so that they can observe and report on any anomalies or suspicious activities. The Security Standard, Section PE-6, requires that an agency monitor physical access to information systems and respond to physical security incidents.

Taxation was unable to meet these security requirements due to lack of dedicated IT Security resources. Taxation did not allocate the resources necessary to identify and respond to the security risks associated with physical access to the server rooms.

We recommend that Taxation dedicate the necessary resources and staff to develop and implement appropriate policies and procedures to protect sensitive IT systems for human risk and in accordance with the Security Standard. We also recommend that Taxation train the affected employees in establishing and reviewing physical access controls to ensure compliance with its own policy and the Security Standard.

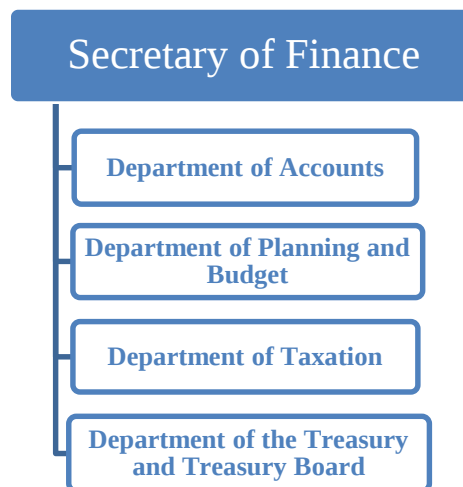
FINANCE SECRETARIAT OVERVIEW

The Departments of Accounts, Planning and Budget, Taxation, and the Treasury and the Treasury Board report to the Secretary of Finance. The individual audits of these agencies primarily support the audit of the Commonwealth's CAFR for the fiscal year ended June 30, 2014, and this report is intended to report on the results of this work.

Our office also issues other reports related to activities or agencies under the Secretary of Finance, these include:

- The "Governor's Cabinet Secretaries" report, which summarizes activities of the Cabinet Secretaries, including the Secretary of Finance. We expect to issue this report in Spring 2015.
- The "Statewide Performance Measures" report, which summarizes work on performance measures reported on the Virginia Performs website, which Planning and Budget maintains. We expect to issue this report in Summer 2015.

The Secretary of Finance (Secretary) assists the Governor in the management and direction of the finance agencies and performs program coordination, policy planning, and budget formulation activities. To accomplish this, the Secretary oversees the following agencies, which perform critical functions in the Commonwealth's statewide financial management system.



These four agencies work closely together in the budgeting, management, and reporting of the Commonwealth's financial resources. They handle all the financial transactions of the Commonwealth from collecting taxes to paying bills to distributing aid to localities. Their primary responsibilities include:

- forecasting and collecting revenues;
- preparing and executing the Commonwealth's budget;
- managing the Commonwealth's cash and investments;
- issuing bonds on behalf of various boards and authorities;
- administering the Commonwealth statewide accounting and payroll systems;
- overseeing the Commonwealth's financial reporting processes; and
- making strategic financial plans.

These agencies primarily serve other agencies within the Commonwealth in a central support capacity. A more detailed discussion of these activities is included in Appendix A along with the interaction of the agencies within the Finance Secretariat while performing these activities.

The operations of these four agencies are primarily funded with general funds. Table 1 summarizes the original and final operating budgets, as well as expenses for all finance agencies except the Treasury Board. The Treasury Board's financial activity is not included since its activities consist primarily of the payment of debt service on general obligation debt rather than administrative expenses.

Table 1 - Summary of Budget and Expenses for Fiscal Year 2014

	Original Budget	Final Budget	Expenses
Secretary of Finance	\$ 425,362	\$ 1,301,939	\$ 1,199,538
Department of Accounts	11,669,654	51,947,346	44,867,443
Department of Planning and Budget	7,314,064	7,727,291	6,547,033
Department of Taxation	98,654,565	102,699,169	98,836,338
Department of the Treasury	<u>18,504,875</u>	<u>19,729,709</u>	<u>18,961,675</u>
Total – Finance Agencies	<u>\$136,568,520</u>	<u>\$183,405,454</u>	<u>\$170,412,027</u>

Source: Commonwealth Accounting and Reporting System

The most significant budgetary changes within the Finance agencies took place in Accounts. Additional positions and funding were provided and used for the implementation and maintenance of various statewide systems, such as Cardinal, Performance Budgeting, and Time, Attendance and Leave. To support the increase in costs, internal service funds were established which are financed from charges to agencies for the use of these systems, including the recovery of development and implementation costs initially funded through working capital advances.

Additionally, the budget for the Secretary of Finance increased during the year due to a general fund transfer from the Federal Action Contingency Trust (FACT) fund. These funds were given to grant recipients to offset the potential loss of any revenue to the Commonwealth caused by federal budget reductions.

The majority of expenses in the Finance Secretariat are for personal services (approximately 50 percent) and contractual services (approximately 44 percent). Table 2 summarizes the type of expenses each of the Finance Secretariat agencies incurred during fiscal year 2014.

Table 2 - Summary of Expenses by Type for Fiscal Year 2014

	Secretary of Finance	Accounts	Planning and Budget	Taxation	Treasury
Personal services	\$ 408,802	\$12,048,632	\$5,015,714	\$59,856,516	\$ 8,543,358
Contractual services	4,995	31,573,127	1,169,430	32,506,626	9,031,181
Supplies and materials	780	69,277	15,399	321,511	308,745
Transfer payments	750,000	2,963	503	96,419	217,706
Continuous charges	32,490	1,070,544	317,875	4,191,084	806,125
Equipment	2,471	101,271	28,112	1,864,182	54,560
Other	-	1,629	-	-	-
Total expenses	<u>\$1,199,538</u>	<u>\$44,867,443</u>	<u>\$6,547,033</u>	<u>\$98,836,338</u>	<u>\$18,961,675</u>

Source: Commonwealth Accounting and Reporting System

Retail Sales and Use Tax Collection and Distribution

In accordance with Section 30-133.2 of the Code of Virginia, we perform work related to retail sales and use tax distributions as part of our annual audit of Taxation. Our previous review, issued in September 2013, covered retail sales and use tax with a focus on the collection and distribution of local sales and use taxes. As part of this review, we reviewed activity for fiscal years 2009 through 2012 and established a benchmark by which to evaluate errors in the process.

In fiscal year 2014, Taxation collected approximately \$5.5 billion in retail sales and use taxes, with \$1 billion of these revenues being distributed to localities as a one percent local option tax. Taxation collects the tax and determines the local portion which is distributed to the locality where the sale or activity occurred.

The sales and use tax distribution process requires a joint effort between Taxation, localities, and businesses. There are a number of controls and processes in place to help ensure that locality distributions are accurate and made to the correct locality. When an error is detected, Taxation processes an adjustment to correct the distribution and transfer the funds to the correct locality.

Table 3 shows the local distribution amount for retail sales and use tax, as well as the amount and rate of distribution errors identified and corrected by Taxation in each of the last three fiscal years.

Table 3 - Error Rate for Local Sales Tax Distributions

	2012	2013	2014
Local Distribution Amount	\$1,052,521,923	\$1,089,743,109	\$1,094,793,721
Errors Identified and Corrected	5,725,742	5,640,689	5,067,477
Error Rate	0.54%	0.52%	0.46%

Source: Taxation's Integrated Revenue Management System

As shown above, the error rate for 2014 was .46 percent; this is well within the one percent benchmark established in our earlier review. Based on these results, it appears that Taxation is properly distributing the local portion of the retail sales and use tax and we do not recommend any changes in the established benchmark.



Martha S. Mavredes, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

January 26, 2015

The Honorable Terence R. McAuliffe
Governor of Virginia

The Honorable John C. Watkins
Chairman, Joint Legislative Audit
and Review Commission

We have audited the financial records and operations of the agencies under the **Secretary of Finance** for the year ended June 30, 2014. 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 primary audit objectives for the audit of the Departments of Accounts, Planning and Budget, Taxation, and Treasury for the fiscal year ended June 30, 2014, include the following:

- to determine whether management has established and maintained internal controls over the Commonwealth's financial reporting and other central processes and the centralized services provided to agencies and institutions in support of the preparation of the financial statements as indicated in the scope section of this report;
- to determine whether management has established and maintained adequate operating and application system controls over CARS, CIPPS, FAACS, LAS, the Integrated Revenue Management System, the Performance Budgeting System, and other central systems;
- to evaluate the accuracy of financial transactions related to the processing of payroll and leave activity by Accounts' Payroll Service Bureau;

- to evaluate the accuracy of financial transactions related to tax collections including accounts receivable, deferred revenues and taxes, accounts payable and other liabilities, and tax and interest revenue as reported in CARS and the Integrated Revenue Management System and in supplemental information prepared by Taxation;
- to evaluate the accuracy of financial transactions related to cash and cash equivalents, investments, debt, risk management, and unclaimed property activity which is controlled by Treasury as reported in CARS and Treasury's accounting records, and in supplemental information prepared by Treasury (including the activity of the Treasury Board, the Local Government Investment Pool, the Virginia College Building Authority, the Virginia Public School Authority, and the Virginia Public Building Authority);
- to evaluate whether the budget approved by the General Assembly is appropriately recorded in CARS and controls in CARS are adequate to ensure program expenses do not exceed appropriations;
- to evaluate the proper approval and documentation of administrative budget adjustments;
- to evaluate the accuracy of financial and budgetary transactions of the administrative activities as reported in CARS for certain agencies included in the Secretary of Finance;
- to determine whether the agencies have complied with applicable laws, regulations, contracts and grant agreements; and
- to review corrective actions related to audit findings from the prior year report.

Audit Scope and Methodology

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 and regulations.

We reviewed and gained an understanding of the overall internal controls, both automated and manual, sufficient to plan the audit. We considered materiality and risk in determining the nature and extent of our audit procedures. Our review encompassed controls over the following processes and systems.

Department of Accounts

Financial Reporting*
Payroll Service Bureau Activities
Commonwealth Accounting and Reporting System (CARS)
Commonwealth Integrated Payroll/Personnel System (CIPPS)
Fixed Asset Accounting and Control System (FAACS)
Lease Accounting System (LAS)

Department of Planning and Budget

Performance Budgeting System
Budget Execution

Department of Taxation

Financial Reporting
Tax Return Processing
Tax Revenue Collections
Integrated Revenue Management System

Department of the Treasury (including Treasury Board operations)

Financial Reporting*	Bank Reconciliation System
Bond Issuance	Trust Accounting
Debt Service Expenses	Check Processing System
Investment Trading	Risk Management Claim System
Investment Accounting	Unclaimed Property Management System
Investment Accounting System	Administrative Activities
Securities Lending Transactions	

*including preparation of the Comprehensive Annual Financial Report and Schedule of Expenditures of Federal Awards by Accounts and the preparation of financial statements of the Local Government Investment Pool, the Virginia College Building Authority, the Virginia Public Building Authority, and the Virginia Public School Authority by Treasury.

We performed audit tests to determine whether 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 agencies' operations. We tested transactions and performed analytical procedures, including budgetary and trend analysis.

Audit Conclusions

We noted no matters involving internal controls related to the Commonwealth's financial reporting and central processes and the centralized services provided to agencies and institutions in support of the preparation of the financial statements as indicated in the scope section of this report.

We noted certain matters at Accounts, Planning and Budget, and Taxation involving internal control and compliance with applicable laws and regulations that are required to be reported under Government Auditing Standards related to operating and application system controls of central systems, which are described in the findings entitled "Improve Controls over Cardinal Security," "Improve Payline Web Application and SQL Server Database Security," "Improve Risk Management and Continuity Planning Documentation," "Improve IT Security Audit Plan," "Improve Internal Controls over System Access," "Enhance Performance Budgeting System Access Reviews," "Improve IT Risk Management and Disaster Recovery Planning Programs," "Improve Internal Controls over Advantage Revenue Access," "Update IT Risk Management Plans," and "Improve Physical Security to Server Rooms" in the section entitled "Internal Control and Compliance Findings and Recommendations."

We found that Accounts' Payroll Service Bureau properly stated, in all material respects, the financial records reviewed in support of payroll and leave activity.

We found that Taxation properly stated, in all material respects, the financial records reviewed in support of the tax collections activity detailed in the audit objectives as reported in CARS, the Integrated Revenue Management System, and supplemental information.

We found that Treasury properly stated, in all material respects, the financial records reviewed in support of the cash and investments, securities lending, debt, risk management and unclaimed property activity reported in CARS, Treasury's accounting records, and supplemental information.

We found that the budget approved by the General Assembly is appropriately recorded in CARS, and controls in CARS were adequate to ensure program expenses do not exceed appropriations.

We found that administrative budget adjustments were properly approved and documented.

For the agencies specified in the scope section of this report, we found they properly stated, in all material respects, the financial and budgetary transactions related to their administrative activities recorded and reported in CARS. The financial information presented in this report related to the administrative activities of the agencies came directly from CARS and is recorded 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 agencies of the Secretary of Finance have taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this report.

Exit Conference and Report Distribution

We discussed this letter with management of the respective agencies of the Secretary of Finance and have included their response at the end of this report. We did not audit management's response and, accordingly, we express no opinion on it.

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

AUDITOR OF PUBLIC ACCOUNTS

lcw/clj

Appendix A

This Appendix includes more detailed information on the various services, programs, and activities managed by the agencies in the Finance Secretariat.

Planning, Budgeting, and Evaluation Services

Planning and Budget aids in the development and administration of the state budget, ensuring that agencies conduct their activities within fund limitations provided in the Appropriation Act and in accordance with gubernatorial and legislative intent. Planning and Budget relies on information from all agencies and universities in developing revenue estimates and expense budgets. Accounts provides Planning and Budget with information regarding unspent balances and carry forward amounts. Taxation develops the General Fund revenue forecast due to the fact that the largest source of revenue for the Commonwealth is individual and fiduciary income taxes and state sales and use taxes. Taxation also develops the revenue forecasts for certain non-general fund revenues, which are primarily transportation-related.

Once the General Assembly and the Governor have approved the budget, Planning and Budget provides an electronic copy to Accounts to upload into the Commonwealth Accounting and Reporting System (CARS). CARS contains automated edit controls to ensure agencies do not exceed the spending authority established in the budget.

Throughout the year, Planning and Budget, along with the Governor, has certain statutory authority to increase, decrease, or transfer funds and personnel positions within constraints set forth in the Act. Planning and Budget and Accounts jointly ensure that CARS properly reflects these adjustments. During fiscal year 2014, over 3,000 administrative adjustments were processed by Planning and Budget resulting in a \$4.2 billion increase to the Commonwealth's operating budget as shown in the chart below. These adjustments typically represent additional funding received, transfers between programs, sum sufficient amounts, or any other routine budget adjustments that are processed by the agency and/or Planning and Budget during the fiscal year.

Revenue Administration Services

Taxation administers and enforces the tax laws of the Commonwealth. Due to its tax return processing duties, Taxation is the single largest collector of Commonwealth revenue, which it primarily deposits to the General Fund. During fiscal year 2014, Taxation collected \$15.8 billion in net revenue, depositing \$15.3 billion into the General Fund. In addition, both Taxation and Accounts collect money owed to the Commonwealth through a debt set-off program that they jointly administer in accordance with the Code of Virginia's Debt Collection Act.

Taxation also collects and distributes Communication Sales and Use Tax to localities and members of the transportation districts as required by the Code of Virginia. During fiscal year 2014, Tax distributed \$422.8 million of Communication Sales and Use Tax revenues.

Check Processing and Bank Reconciliation

Treasury prints and distributes all Commonwealth of Virginia check disbursements, including vendor payments, social service, payroll, and tax refunds. Treasury also reconciles all Treasurer of Virginia bank accounts within 45 days of month end as required by the Code of Virginia. This includes approximately seventy bank accounts including the Commonwealth's large concentration bank accounts, disbursing accounts, and regional depository accounts.

Unclaimed Property Administration

Additionally, under the Unclaimed Property Act, Treasury serves as custodian of certain personal properties (intangible and tangible personal property) until the Commonwealth can locate the owner. Treasury identifies abandoned personal property through annual reporting requirements and the performance of audits and compliance reviews, administers the fund under the Commonwealth's control, and uses its best efforts to return the property to its owner.

Investment, Trust, and Insurance Services

Treasury, under the direction of the State Treasurer, invests the Commonwealth's funds and provides trust and insurance services. Treasury manages and invests the Commonwealth's funds throughout the year striving to preserve capital and liquidity while earning the best possible return, in accordance with Treasury Board approved investment guidelines. The largest portfolio Treasury manages is the General Account of the Commonwealth, a pool of investments representing assets of the Commonwealth's General Fund, highway maintenance, and transportation trust funds. The General Account has two portfolios: the primary liquidity portfolio and the extended duration and credit portfolio. Treasury internally manages the primary liquidity portfolio, which provides the major source of liquidity for the disbursement requirements and operational needs of the Commonwealth. The externally managed "Extended Duration and Credit Portfolio" seeks to generate higher total returns over time. Treasury's target allocation for the overall general account asset mix is 75 percent for the primary liquidity pool and 25 percent for the total return pool.

Treasury also manages the Local Government Investment Pool (LGIP), a short-term investment pool offered to counties, towns, cities, state agencies, departments, and authorities of the Commonwealth of Virginia. It is an open-ended money market type fund that offers public funds investors daily liquidity, diversification, and professional management. Further, Treasury manages the Commonwealth's statewide banking network and monitors its own and other agencies' specialized banking services.

Treasury is also responsible for the issuance and management of debt of the Commonwealth and several of its boards and authorities. Treasury provides staff support to the Virginia Public School Authority, the Virginia College Building Authority, the Virginia Public Building Authority, the Debt Capacity Advisory Committee, the Tobacco Settlement Financing Corporation, and the Treasury Board.

Finally, Treasury administers insurance programs on behalf of the Commonwealth that cover state government, other public entities, and certain individuals serving in the public interest. Administered insurance programs are either self-insured, commercially insured, or are a combination of both. Treasury bills state agencies, the Compensation Board, and local governments for insurance premiums to cover current and future costs. Types of insurance include property, auto liability, medical malpractice, general liability, and fidelity bonds.

We performed an audit of the financial activity of the Local Government Investment Pool, the Virginia College Building Authority, the Virginia Public School Authority, and the Virginia Public Building Authority for the year ended June 30, 2013, and reported our audit results in a separate audit report issued in January 2014.

Treasury Board

The Code of Virginia sets forth the appointments to the Treasury Board, which includes the State Treasurer, the State Comptroller, the State Tax Commissioner, and four members appointed by the Governor. Treasury provides support services to the Treasury Board in fulfilling its responsibilities, which include the following.

- Exercise general supervision over the investment of state funds
- Administer the Virginia Security for Public Deposits Act
- Control and manage sinking and other funds that the Commonwealth holds as fiduciary
- Contract with an outside manager for the administration of the State Non-Arbitrage Program
- Provide advice and supervision in the financing of state buildings
- Approve the terms and structure of proposed state educational institution bond issues and other financing arrangements
- Approve the terms and structure of proposed bond issues secured by state appropriations
- Administer the regional jail financing reimbursement program
- Issue all general obligation debt of the Commonwealth
- Manage its bond issues in compliance with federal taxation and arbitrage laws

In addition, the Treasury Board makes payments for the Virginia College Building Authority and the Virginia Public Building Authority for lease payments and/or bond principal and interest on the Authorities' appropriation-supported debt. The Board also pays debt service on Article X, Section

9(b) general obligation bonds and processes debt service payments to trustees and/or paying agents on behalf of the Commonwealth Transportation Board.

Financial Systems Development and Management

Accounts operates and maintains the Commonwealth's centralized automated accounting, payroll, and fixed asset systems. CARS is a cash-basis accounting system that records all of the Commonwealth's cash receipts and disbursement transactions and provides a means to enforce state appropriation law for all state agencies through automatic edits and manual reviews. The Commonwealth Integrated Payroll/Personnel System (CIPPS) is the Commonwealth's central payroll and leave system. Agencies and institutions use CIPPS to process employee salaries and wages, tax computations, payroll deductions, and leave transactions. The Fixed Asset Accounting and Control System (FAACS) and Lease Accounting System (LAS) record the Commonwealth's capital and controllable assets and equipment leases.

Accounting Services

To facilitate the operation of CARS, CIPPS, FAACS, and LAS, Accounts has developed policies and procedures for entering transactions in the systems and offers periodic training courses to other agencies. In addition, Accounts grants access to the systems, monitors activity in the systems, provides assistance to agencies on financial reporting issues, performs reconciliations, and resolves errors as necessary.

Accounts processes certain transactions in CARS including reoccurring or correcting journal entries, transfers as required by the Appropriation Act, and the quarterly calculation and allocation among the various funds of interest earned by Treasury on the Commonwealth's cash and investments. Accounts is responsible for all aspects of the payroll process including payroll production, payroll and benefits accounting, and compliance with state and federal tax regulations.

Accounts calculates and distributes certain revenues collected by Taxation to local governments as required by the Code of Virginia. The Appropriation Act budgets and Accounts records these transfer payments under agency 162, Department of Accounts Transfer Payments. Accounts distributed the following amount of revenue during fiscal year 2014.

Sales and use tax for education	\$1,206,921,885
Personal Property Tax Relief Act	950,000,000
Recordation taxes	19,920,903
Other	<u>2,711,189</u>
Total	<u><u>\$2,179,553,977</u></u>

Source: Commonwealth Accounting and Reporting System

Accounts also made recordation tax transfers to the Department of Transportation for the Northern Virginia Transportation District Fund and the Transportation Improvement Set-Aside Fund in the amounts of \$18,996,800 and \$1,082,295, respectively.

Another accounting services item Accounts completes is the preparation of several key reports used to monitor the Commonwealth's activity throughout the year and report year-end results. The other agencies within the Finance Secretariat contribute to this process due to the significance of their roles in the budgeting and financial management activities of the Commonwealth.

During the year, the Commonwealth monitors its General Fund revenue collections using the Monthly Revenue Report, which the Secretary of Finance issues. Accounts accumulates the financial information for this report from CARS and various agencies. Taxation provides Accounts with the General Fund revenue forecast for the report and provides detailed information on certain actual revenue collections. Treasury provides Accounts with information on the Commonwealth's investing activity.

At year-end, Accounts prepares two reports: The General Fund Preliminary Report and the Comprehensive Annual Financial Report (CAFR). Accounts prepares the General Fund Preliminary Report using CARS financial activity and information provided by Planning and Budget for the classification of remaining General Fund balances. Accounts prepares the CAFR using financial activity recorded in CARS as well as information submitted by agencies. Due to the significance of the activity controlled by Taxation and Treasury, these agencies must work closely with Accounts in providing the information necessary to prepare the CAFR. To ensure accuracy of the data in the General Fund Preliminary Report and CAFR, the Financial Reporting division of Accounts performs periodic quality assurance reviews of agency submitted information.

Other reports prepared throughout the year include the Popular Annual Financial Report, the federal and full-costing Statewide Indirect Cost Allocation Plan, and the Statewide Schedule of Expenditures of Federal Awards.

Service Center Administration

The Payroll Service Bureau division of Accounts processes payroll, leave accounting, and certain benefits data entry functions for selected agencies. Additionally, the Finance and Administration Division of Accounts provides services for selected agencies, including processing payroll, vendor payments, and revenues.



COMMONWEALTH of VIRGINIA

DAVID A. VON MOLL, CPA
COMPTROLLER

Office of the Comptroller

P. O. BOX 1971
RICHMOND, VIRGINIA 23218-1971

February 4, 2015

Ms. Martha S. Mavredes
Auditor of Public Accounts
James Monroe Building
101 N. 14th Street
Richmond, Virginia 23219

Dear Ms. Mavredes:

The Department of Accounts (Accounts) appreciates the opportunity to respond to the *Comments to Management* contained in your 2014 Secretary of Finance Audit Report. We give your comments the highest level of importance and consideration as we continue to review and improve our current practices. Accounts appreciates your acknowledgement of the progress made and the recognition that some issues take significant time and resources to resolve.

Comments to Management

Modernization of Financial Reporting Processes

Accounts appreciates the recognition that the financial reporting landscape is changing and that additional process changes are required to successfully navigate additional reporting complexities arising from new accounting standards, laws and regulations while facing decreasing numbers of financial reporting staff in the Commonwealth. Accounts' General Accounting and Financial Reporting Divisions are striving to identify new systems applications or changes to existing applications in order to evaluate the appropriate accounting and reporting treatment. Additionally, the Financial Reporting Division has incorporated, and continues to explore the expanded use of, databases into the current reporting process. Accounts will continue using a risk-based approach when evaluating agency financial information. The Finance and Administration Division will continue to evaluate both efficiency and effectiveness of agency processes when performing agency quality assurance reviews. Accounts will strengthen partnership arrangements with line agencies to facilitate the agencies' understanding and process improvements. Accounts will continue to evaluate the best means of communicating with agencies and provide comprehensive policies and procedures governing the Cardinal operation prior to implementation.

Statewide Implementation of New Federal Grant Requirements

Accounts agrees that the Office of Management and Budget's (OMB) Uniform Guidance: Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (Uniform Guidance) represents a significant change in federal reporting and will require evaluation of the current Commonwealth processes. As noted in the report, Accounts will communicate information to the fiscal

(804) 225-2109

FAX (804) 786-3356

TDD (804) 371-8588

officers to ensure they are aware of the reporting requirements and can implement the necessary action to comply with the Uniform Guidance.

Upcoming Pension Accounting Changes

As noted, the newly issued Governmental Accounting Standards Board standards for accounting and reporting pension activity for state and local governments will change the way the Commonwealth and localities compute and report pension obligations. Accounts will work with the Virginia Retirement System to implement necessary changes to the Commonwealth's financial statements in fiscal year 2015.

Ensure Accurate Management of Member Data by Agencies

Accounts recognizes the necessity to increase the Commonwealth's financial community's awareness of the importance of accurate member data. To help facilitate this increased awareness, Accounts will update the Commonwealth Accounting Policies and Procedures Manual topic concerning VRS Retirement and post this on Accounts' website. Additionally, the Payroll Service Bureau within Accounts will enhance the *Business Process Overview* to clearly outline the processes the Bureau uses in regards to the VRS Reconciliation.

Internal Control and Compliance Findings and Recommendations

Improve Controls over Cardinal Security

Accounts recognizes the need to suspend access for dormant users in Cardinal. Accounts will implement a process to both identify and suspend access once a user account has been dormant for 90 days. Additionally, Accounts agrees that there are instances in Cardinal where the same individual user can both enter and approve the same transaction. However, this capability, as developed and built by the software provider, is limited only to adjusting journal entries in the journal module. Accounts is extremely disciplined with regard to customizations to the delivered software in order to reduce the risk and cost associated with the implementation of planned software upgrades in the future. It should be noted that this security capability is not available in any of the modules that result in a disbursement of cash from the state treasury. All transactions resulting in the disbursement of cash have the delivered systemic control of not allowing the same individual to both enter and approve the transactions. Accounts acknowledges that allowing the same individual user to both enter and approve a financial transaction is not consistent with general best practices surrounding system security. However, given that this capability is restricted to adjusting journal entries, Accounts believes the risk is very limited and can be effectively mitigated by the reconciliations performed by agencies and by utilizing the available process to specifically identify and monitor adjusting journal entries entered and released by the same individual user timely. Accounts will implement this specific identification and monitoring process immediately.

Improve Web Application and SQL Server Database Security

Accounts recognizes the need to improve security controls to reduce the unnecessary risk to data confidentiality, integrity and availability of sensitive data. Accounts has taken the steps necessary to address the five control weaknesses communicated to Accounts management in the document marked Freedom of Information Act Exempt under Section 2.2-3705.2 of the Code of Virginia. Additionally, Accounts has dedicated the newly hired Information Security Specialist and other technical resources to implement the security controls discussed in the communication marked FOIA-Exempt in accordance with the Commonwealth's IT Security Audit Standard, SEC501-07.1.

Improve Risk Management and Continuity Planning Documentation

Accounts recognizes and understands the requirements to ensure that the agency's framework documentation is current and compliant. Accounts has made significant gains in documenting the sensitive business processes and associating applications within the Business Impact Analysis and Risk Assessments. Although not complete, Accounts will dedicate the necessary resources to complete the agency's Business Impact Analysis and Risk Assessment plans accordingly and incorporate the findings into the COOP/DRP plans. This will be an ongoing process with the introduction of new business application processes.

Improve IT Security Audit Plan

Accounts recognizes the importance of having the agency's framework documentation kept up to date and as current as possible. Accounts has made significant gains in documenting the sensitive business processes and associating applications within the Business Impact Analysis and Risk Assessments. Although not complete, Accounts will dedicate the necessary resources to complete the agency's Business Impact Analysis and Risk Assessment plans accordingly as well as incorporate the updated plans into the three year audit plan as recommended by Commonwealth Security Standards and industry best practices.

Sincerely,



David A. Von Moll

Copy: The Honorable Richard D. Brown, Secretary of Finance
Lewis R. McCabe, Jr., Assistant State Comptroller – Accounting & Reporting



COMMONWEALTH of VIRGINIA

Department of Planning and Budget

DANIEL S. TIMBERLAKE
Director

1111 E. Broad Street
Room 5040
Richmond, VA 23219-1922

January 14, 2015

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

Dear Ms. Mavredes:

Thank you for the opportunity to provide the Department of Planning and Budget's (DPB's) response to the findings identified as part of your audit of this department's financial records and operations for the year ended June 30, 2014.

As requested by your office, this letter provides a response to each of the three management recommendations along with a corrective action plan for each recommendation. I also want to take this opportunity to provide you with my general comments regarding the three recommendations.

I would like to thank your office for taking the time to meet and discuss these recommendations with me in November of 2014. The discussion was helpful to me as DPB gives careful consideration to these recommendations and acknowledges that this agency, and every state agency for that matter, needs to continue to strengthen its internal controls. DPB recognizes that opportunities exist to document current policies related to the Performance Budgeting (PB) System, and we will enhance and supplement the direction provided to state agencies. In response to your recommendations and to discussions that took place during the audit, DPB is also actively working with the Virginia Information Technology Agency (VITA) and with other finance agencies to find cost-efficient options that will address the Commonwealth's Security Standard.

While I appreciate the acknowledgement in your recommendations that PB system transactions do not impact the Commonwealth's Accounting system until several layers of review and approval have taken place at DPB, I am concerned that your recommendations do not adequately reflect the current safeguards that exist in this system. The PB financial system is a means to allow agencies to request budget execution actions and budget amendments. In the November meeting and in information provided by my staff as part of the audit, DPB indicated that no transaction entered into the PB system is processed until an internal review is undertaken at this agency. Depending upon the nature of the transaction, that review could involve multiple layers and could even require my review and approval. No transaction is approved in the PB system until it undergoes this process, which includes validating the identity of the individual(s) at a state agency who enter and review a transaction in the PB system.

FAX (804) 225-3291

(804) 786-7455

TDD (804) 786-7578

System safeguards also exist through limiting the actions that a state agency user is able to perform. For state agency users, the PB system acts as a “portal” for submitting budget requests. The PB system functions much like a website for soliciting public requests; however, since the requests are from state agencies, DPB allows state agencies to determine the personnel who should access this system and the degree to which access should be limited. The risk of misuse is no greater than the risk that would exist if DPB received such requests as paper submissions. Therefore, the current procedures in place for the PB system inherently mitigate opportunities for misuse of the system by state agency personnel.

I also note that the two management recommendations related to the PB system essentially deal with the same issue and it was my understanding from the November meeting that this consolidation was under consideration. I believe that this consolidation could provide greater clarity as two separate recommendations related to the PB system have the unintended consequence of allowing for an audit form of “double jeopardy.”

In regard to the recommendation related to IT risk management and disaster recovery, DPB gives the highest level of consideration to your comments and recommendations, and I will reiterate that DPB is working with VITA to identify solutions that could be implemented within the resources that currently exist for a small state agency. The solutions identified thus far are costly and represent recurring financial commitments. The recommendation states that DPB should be dedicating the necessary resources to ensure the performance of risk assessments, but I am concerned that the resources that your office expects this agency to dedicate may not be possible because of current and future budgetary constraints. I also want to note that this agency has long-standing staff with IT backgrounds, and the staff closely monitors all of DPB’s systems and works closely with VITA to address any system issues, which include access issues. It is also important to note that, when VITA was formed, staff and resources to perform these functions were removed from state agencies and transferred to VITA. As time has passed, VITA has not taken on the role of providing security services for agency-based legacy systems nor has funding been restored to agencies to resume these responsibilities.

Improve Internal Controls over System Access - Performance Budgeting (PB) System

In response to this management recommendation, DPB will ensure that formal policies and procedures are prepared and updated and state agencies will be provided with information regarding user role capabilities within the PB system. The development plan for this finding will be completed no later than October 31, 2015.

Enhance Performance Budgeting System Access Reviews

In response to this management recommendation, DPB will revise its annual review process related to PB system access to incorporate the following: 1) positive confirmation that all agency access continues to be appropriate and necessary; 2) an internal review process to assess the number of agency administrators in relation to the size and nature of the agency; and 3) an annual review process that identifies any unresponsive agencies. The development plan for this finding will have a completion date of August 31, 2015. Please note that any system changes needed to address this finding must be implemented with existing resources.

Ms. Martha Mavredes
January 14, 2015
Page Three

Improve IT Risk Management and Disaster Recovery Planning Programs

In regard to its Disaster Recovery Plan (Plan), DPB will review this plan in conjunction with its annual update of the Continuity of Operations Plan (COOP) to ensure that the Plan addresses annual exercises of effectiveness. As part of this review, DPB will formalize in the COOP and its Plan the existing process where the PB system is periodically subject to software updates where the system is brought down and then restored. DPB also will work with VITA to meet the Commonwealth's Security Standard. The development plan for this finding will have a completion date of August 31, 2015, and I note that the plan will be developed within the constraints of existing financial resources.

Sincerely,



Daniel S. Timberlake

c: The Honorable Richard D. Brown



COMMONWEALTH of VIRGINIA

Department of Taxation

January 21, 2015

Ms. Martha S. Mavredes
Auditor of Public Accounts
James Monroe Building
101 N. 14th Street
Richmond, Virginia 23219

Dear Ms. Mavredes:

The Department of Taxation has reviewed the findings and recommendations provided by the Auditor of Public Accounts as part of your audit of the Department's financial records and operations for the year ended June 30, 2014. I appreciate the effort and professionalism of your staff engaged in the audit this year and provide the following responses to address the report findings.

Improve Internal Controls Over Systems Access

I appreciate that the auditor's comments acknowledge that compensating controls exist for the identified weaknesses and that no instances of unauthorized transactions were identified. I would also note that the journal vouchers noted in the comment, in addition to not being material, do not update the Commonwealth's accounting system and are only an internal reconciling aid.

Those clarifications aside, the Department will initiate the following actions to address the issues noted in the comment:

1. Approvers will no longer edit and approve the same transaction. There is also a compensating control whereby the agency's financial balances are compared to the commonwealth's financial balances.
2. The Department's Internal Audit will compare a history of critical access capabilities in Advantage Revenue application to critical accesses performed, to identify employees with potentially unnecessary access, and challenge the employee's access to this capability.
3. Technology staff will reconcile the user access noted in the system of record to the system of documentation.

Save Time, Go Online - Visit www.tax.virginia.gov

4. Technology staff will revise access documentation for the Advantage Revenue application so that management and employees are better informed of the privileges associated with access levels.
5. Management will recertify that their employee's access is required for current job requirements.

The development plan for this finding will have a completion date of September 30, 2015.

Improve IT Risk Management Plans

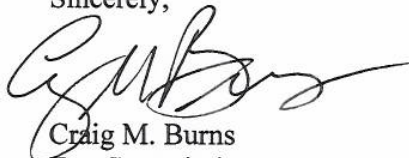
The Department recognized these planning and documentation issues and requested funding to hire qualified staff to address these issues. The 2014 General Assembly approved the requested funding and the Department has hired an Information Technology Risk Manager and three other IT security positions are being recruited. The Risk Manager will be responsible for preparing the update to the agency's BIA and Risk Assessment. The development plan for this finding will have a completion date of September 30, 2015.

Improve Physical Security to Server Room

Annually, Department supervisors perform a recertification of all physical access permissions. We will add a step to the recertification procedures that requires the supervisors to document in the employees' Employee Work Profile forms the purpose for any "special access." In addition, we will assign responsibility for the review of the physical access daily activity logs to a staff person who does not have access to these facilities. The development plan for this finding will have a completion date of September 30, 2015.

Again, thank you for the opportunity to respond to your report. The Department strives to maintain strong internal controls and business processes that ensure high standards of integrity, efficiency, and control. Completely addressing your report findings will assist us in this endeavor.

Sincerely,



Craig M. Burns
Tax Commissioner

c: The Honorable Richard D. Brown, Secretary of Finance

SECRETARY OF FINANCE AGENCY OFFICIALS

As of June 30, 2014

Richard D. Brown
Secretary of Finance

David A. Von Moll
Comptroller

Daniel S. Timberlake
Director of the Department of Planning and Budget

Craig M. Burns
Tax Commissioner

Manju S. Ganeriwala
Treasurer