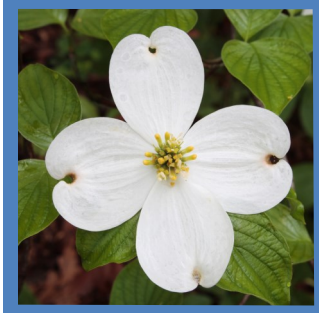

SECRETARY OF FINANCE

REPORT ON AUDIT
FOR THE YEAR ENDED
JUNE 30, 2015

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

AUDIT SUMMARY

This report summarizes our fiscal year 2015 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, 2015, 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 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 of the implementation occurred in two waves. Wave 1 involved agencies who directly key transactions into Cardinal, and this was completed in October 2014. Wave 2 involves agencies who interface data from their independent financial system into Cardinal and this final stage is on schedule for completion by February 2016. Cardinal will become the official system of record by the beginning of fiscal year 2017 with the retirement of the existing CARS financial system.

–TABLE OF CONTENTS–

SIGNIFICANT INITIATIVES

The following section provides updates on major Commonwealth initiatives affecting Secretary of Finance agencies.

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) beginning in fiscal year 2017. The project is in its final phase of statewide agency roll-out, with all agencies on schedule to be live with Cardinal by February 2016.

This is a key project since the current accounting system is outdated both in terms of the technology and available functionality.

Cardinal's base modules provide the foundation for a modern financial system for the Commonwealth with the ability to add other modules and expand functionality in future projects. As an example, the Department of Accounts (Accounts) has initiated project planning to replace the aging statewide payroll system (CIPPS) with Cardinal's Human Resource and Payroll modules.

Our December 2015 report, "Governance over Enterprise Applications," describes how agencies that manage existing statewide applications have authority to determine when to replace a system, what system to use, and how the system will function. In our report, we recommend this process be improved through the creation of an enterprise governance structure that would allow executive branch leadership to collaborate on statewide application decisions to ensure that the software selections promote government interoperability and support the Commonwealth's strategic plan. In addition, the enterprise governance structure would be a good resource to identify other future Cardinal service offerings, which if implemented, would allow agencies to retire their independent financial systems and use Cardinal instead.

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. It takes time to implement these changes, and 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.

RISK ALERT

A risk alert differs from an internal control and compliance finding in that it represents an issue that is beyond the corrective action of the individual agency and requires the cooperation of others to address the risk.

Increased Risk to Commonwealth's Applications Running on IT Infrastructure Partnership Servers

The Commonwealth's Information Technology (IT) Infrastructure Partnership with Northrop Grumman (Partnership) provides agencies with installation, maintenance, operation, and support of IT infrastructure components, such as server operating systems, routers, firewalls, and virtual private networks. During our reviews, we found that the Partnership is not maintaining some of these devices according to the Commonwealth's Information Security Standard, SEC 501-09 (Security Standard) and is exposing the Commonwealth's sensitive data to unnecessary risk.

End-Of-Life Systems
(Applicable to Accounts, Treasury, and Taxation)

The Partnership uses end-of-life and unsupported systems in its IT environment to support some of the Commonwealth's mission-critical applications. The Commonwealth relies on the Partnership to provide current, supported, and updated systems that serve as the foundations for their respective mission-critical and sensitive systems. The Security Standard, section SI-2-COV, prohibits the use of products designated as "end-of-life" by the vendor. A product that has reached its end-of-life no longer receives critical security updates that rectify known vulnerabilities that malicious parties can exploit.

The Partnership maintains and administers four server operating systems for the Accounts, four server operating systems for the Department of the Treasury (Treasury), and 20 server operating systems for the Department of Taxation (Taxation) that the respective vendor has designated as end-of-life. The Partnership also uses end-of-life software to administer Taxation's desktop virtualization environment. The Partnership's use of unsupported server operating systems and virtualization software increases the risk that existing vulnerabilities will persist in the systems without the potential for patching or adequate mitigation. These unpatched vulnerabilities increase the risk of cyberattack, exploit, and data breach by malicious parties. Additionally, vendors do not offer operational and technical support for systems designated as end-of-life, which increases the difficulty of restoring system functionality if a technical failure occurs.

Missing Server Operating System Security Patches
(Applicable to Accounts and Taxation)

The Partnership does not perform timely patching of some of the server operating systems that support mission critical systems in the Commonwealth. The Commonwealth relies on the Partnership to provide updated and appropriately patched server operating systems that serve as the foundations for its mission-critical and sensitive systems. The Security Standard, section SI-2-

COV, requires that an organization apply all software publisher security updates to the associated software product as soon as possible after appropriate testing, not to exceed 90 days for implementation.

The Partnership maintains four server operating systems for Accounts and more than 70 server operating systems for Taxation that are not being patched on a timely or consistent basis. The Partnership's inconsistent and non-timely patch management process for the related server operating systems increases the risk that existing vulnerabilities will persist. These unpatched vulnerabilities increase the risk of cyberattack, exploit, and data breach by malicious parties.

Unavailable Server Baseline Configuration Documentation
(Applicable to Taxation)

The Partnership does not share with Taxation how it configures the security settings in the server operating systems used to run Taxation's applications, also known as baseline configuration documentation. Taxation relies on the Partnership to install and configure servers according to a pre-defined baseline configuration standard. However, without both parties agreeing on the same baseline configuration, Taxation cannot properly configure and maintain its applications to ensure compliance with the Security Standard.

The Security Standard, Section CM-2, requires baseline configuration documentation that is consistently used for the installation, update, and configuration of IT systems. Without sufficient baseline configuration documentation, server operating systems will not be consistently configured to meet all the requirements in the Security Standard and industry best practices.

Accounts, Treasury, and Taxation are aware of the unsupported system issues and are working with the Partnership to develop remediation plans to upgrade or decommission the related systems as soon as possible. Accounts and Taxation are also aware of the unpatched server operating systems and are working with the Partnership to develop remediation plans to ensure that the related server operating systems become patched as soon as possible. Additionally, Taxation is further working with the Partnership to ensure that all servers are configured according to a pre-defined baseline configuration standard. Until these weaknesses are mitigated, Accounts, Treasury, Taxation, and the Partnership have installed additional security controls to attempt to reduce some of the risk that the end-of-life server operating systems introduce into the IT Environment.

The Partnership should continue working with Accounts, Treasury, and Taxation to upgrade or decommission all of the end-of life server operating systems as soon as possible. The Partnership should also continue working with Accounts and Taxation to patch all of the server operating systems as soon as possible. Additionally, the Partnership should also improve its established patching procedures to ensure that Commonwealth operating servers do not inappropriately fall behind in the patch management cycle. Further, the Partnership should ensure that all servers are configured according to a pre-defined baseline configuration standard. Doing this will further reduce the risk to the confidentiality, integrity, and availability of sensitive Commonwealth data and achieve better compliance with the Security Standard.

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Department of Accounts

Improve Cardinal System Security Controls

Accounts has not implemented some of the required controls to protect the Cardinal enterprise resource planning system (Cardinal) as required by the Security Standard and industry best practices. Cardinal is a web-based accounting system that is replacing the legacy Commonwealth Accounting and Reporting System (CARS) as the official system of record. Cardinal also processes and stores sensitive data including personally identifiable information.

We identified five internal control weaknesses and communicated them 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.

Accounts should dedicate the necessary resources to provide committed information security oversight for Cardinal. Accounts should also dedicate the necessary resources to timely implement the controls discussed in the communication marked FOIA-Exempt in accordance with the Security Standard and industry best practices.

Continue to Improve Payline Security – Repeat Finding

Accounts continues to not appropriately secure the Payline web application and supporting database in accordance with the minimum security controls required by the Security Standard and industry best practices. Payline is a web-based system that reports the earnings statements for all state employees and contains personally identifiable information.

We identified two control weaknesses and communicated them to management in a separate document marked FOIA Exempt under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. Subsequent to this communication with management, Accounts corrected one of the two weaknesses. The Security Standard requires implementing specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability.

Accounts should continue to dedicate the necessary resources to implement timely the controls discussed in the communication marked FOIA-Exempt in accordance with the Security Standard.

Continue to Improve Risk Management and Continuity Planning Documentation – Repeat Finding

Accounts continues to 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 their BIA or RAs since 2010, and has not updated the COOP and DRP since April of 2013 to reflect their current environment.

The Security Standard requires agencies conduct annual reviews of the BIA and conduct a full revision at least once every three years. Section 6.2 of the Security Standard requires agencies to update their RAs for 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 RAs. Also, the Security Standard, Section 8.6 requires the COOP and DRP to be based on the results of the BIA and RAs. Furthermore, Section 8.6 of the Security Standard requires agencies to update the continuity planning documentation to reflect any material changes to the organization, information systems, operating environment, and problems encountered during continuity plan implementation, execution, or testing.

By not having accurate and updated Risk Management and Continuity Planning documentation, Accounts continues to increase the risk of not being able to appropriately plan for and restore essential business functions and supporting resources currently in place in their environment in the event a disaster occurs and during necessary restoration efforts.

Accounts continues to not perform corrective actions for the weaknesses identified above primarily due to the ongoing development, implementation, and roll out of the new accounting and reporting enterprise management system (ERP), Cardinal. The Cardinal ERP's roll out represents a significant change to Accounts' operating environment in terms of both business process as well as the underlying technology, as it is replacing the legacy Commonwealth Accounting and Reporting System. Cardinal has a planned completion date of February of 2016. Additionally, Accounts is working through a system migration project, in which other sensitive systems are undergoing upgrades that will also significantly affect the documentation of information in the Risk Management and Continuity Planning documents. Based on the new Cardinal system implementation and the system migration project, Accounts continues to delay the necessary corrective actions for updating the Risk Management and Continuity Planning components.

Accounts should continue corrective actions and dedicate the necessary resources to appropriately revise, approve, and test the Risk Management and Continuity Planning documentation per the requirements of the Security Standard.

Continue to Improve IT Security Audit Plan – Repeat Finding

Accounts continues to have an outdated IT Security Audit Plan that is inconsistent with its BIA and RA documents. Also, Accounts continues to not perform IT security audits over IT systems

classified as sensitive to ensure they are reviewed at least once every three years, nor has Accounts 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 (IT Audit Standard), SEC502-02, Section 1.4 and 2.1 requires that:

- Agencies develop and maintain an IT security audit plan for the IT systems for which they are the Data Owner.
- Agencies base their IT security audit plans on the BIA and the systems' data classifications.
- The respective Agency Head submit the updated IT security audit plan to the Commonwealth's CISO on an annual basis.
- IT systems that contain sensitive data be assessed at least once every three years in accordance with the requirements of the Security Standard.

By not having periodic IT Security Audits performed on sensitive systems currently running in its IT environment, Accounts is increasing the risk for system vulnerabilities and threats to go undetected and not reasonably remediated in accordance with the Security and IT Audit Standards.

Accounts has contracted with an external firm to perform the IT Security Audits over sensitive systems. However, Accounts delayed further progress in corrective actions primarily due to the ongoing development, implementation, and roll out of Cardinal, as documented above. Based on the new Cardinal system implementation and the system migration project, Accounts continues to delay the necessary corrective actions for updating the IT Security Audit Plan and performing IT security audits.

Accounts should continue to dedicate the necessary resources to update its IT Security Audit and Risk Management documentation based on the requirements in the Security and IT Audit Standard. Accounts should also submit the necessary documentation to the Commonwealth CISO on an annual basis as required by the IT Audit Standard. Furthermore, Accounts should continue to dedicate the necessary resources to execute IT security audits for all sensitive systems in accordance with the IT Audit Standard.

Department of Planning and Budget

Update Contingency Planning Documentation

The Department of Planning and Budget (Planning and Budget) does not consistently identify Mission Essential Functions (MEFs) in its Contingency Planning documents. Identifying MEFs properly and consistently is essential for defining and assessing risk management policies and procedures and developing plans to ensure business operation continuity.

The Security Standard, Section 8.6, states that agencies should use the information outlined in the BIA and RAs as the primary input for the Continuity and Disaster Recovery documents, which will ensure consistent documentation. However, the MEFs identified in Planning and Budget's BIA are not consistent with the Continuity of Operations Plan (COOP) and Disaster Recovery Plan (DRP), which leads to inconsistent information, such as excluded supporting IT systems and incorrect Recovery Time Objectives.

By having inconsistencies across the Risk Management and Contingency documents, Planning and Budget may not be able to adequately perform critical business processes in the event of a natural disaster, service disruption, or other unplanned interruptions.

Planning and Budget joined the Virginia Information Technologies Agency's Small Agency Information Security Officer program for assistance in identifying and updating the MEFs and supporting IT system information in the Risk Management documentation (BIA and RA) based on a prior management recommendation. However, due to timing, Planning and Budget has not completed updating the Contingency Plans (COOP and DRP) to reflect the updated Risk Management documentation.

Planning and Budget should allocate the necessary resources to review and update the COOP and DRP documents based on the information identified in the BIA and RAs to ensure they are consistent and in accordance with the Security Standard.

Department of Taxation

Improve Administrative Access Controls

Taxation does not have an effective process for reviewing and managing access for accounts with elevated privileges, such as those accounts used by database and system administrators that support Taxation's systems in accordance with the Security Standard.

Taxation does not have a policy or procedure that governs reviews of specific roles and privileges granted to accounts that Taxation uses to administer databases and server operating systems. Taxation has a defined process for reviewing expired accounts at the database level; however, the process does not include a review of the specific roles and privileges the users have been granted. Additionally, Taxation does not remove expired accounts in a timely manner that is consistent with organizational policy.

We identified and communicated several areas of weaknesses to management in a separate document marked FOIA Exempt under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. In general, these areas consisted of four control weaknesses in inappropriate database privileges, three weaknesses in inappropriate server group allocation, and five weaknesses in removal of unused and expired accounts.

While Taxation immediately remedied the weaknesses above, Taxation did not identify and correct the weaknesses prior to our identification during the audit due to an insufficient access review process for administrative accounts at the database and server levels. Taxation does not have a formally approved and documented process to review granted roles, privileges, and user group allocation for accounts with elevated privileges. Additionally, Taxation does not remove expired accounts in a timely manner due to insufficient implementation of the organizational requirement.

Taxation should create and implement a process for managing access privileges for administrative and system accounts at the database and server levels organization-wide. The process should include a periodic review of granted privileges, roles, group allocation, inactive accounts, and system accounts. Accounts that are no longer required should be removed in a timely manner and according to organizational procedures. By implementing sufficient access controls for accounts with elevated privileges, Taxation will be better able to manage the risks and responsibilities associated with administrative accounts.

Continue to Strengthen Controls over Advantage Revenue Access – Repeat Finding

Taxation needs to continue with efforts to strengthen access controls over its Advantage Revenue system. Our prior report identified several issues with system access including inappropriate access, access combinations that caused segregation of duties issues, and inaccurate information in its access management system, SAFE. These weaknesses in access controls impact Taxation's ability to comply with various aspects of the Security Standard, which addresses requirements over information system access controls.

Since our previous report, Taxation has taken a number of steps to address these issues. While some of these issues have been corrected, other corrective actions are ongoing and will take several years to implement. Taxation has taken the following actions to address some of the previous year's issues:

- Taxation has corrected the instances of inappropriate access for two staff in the General Legal and Technical Services section. They have also restricted access to the REV1 workgroup, which controls journal vouchers pending approval, to only the users who require access.
- Taxation has implemented a compensating control to address the lack of segregation of duties created with access to edit and approve journal vouchers. This compensating control is a quarterly review of journal vouchers by Taxation's Internal Audit to ensure the approver does not edit the journal voucher.
- Taxation has improved its access documentation to better reflect access granted by the various security groups by creating Report 521.0. This report is stored in Taxation's reporting tool, Business Objects, and shows access granted by each security group or to each employee. Report 521.0 will now be available for supervisors to run at any time.
- Taxation's Internal Audit department conducted an internal review of Advantage Revenue system access. They reviewed access to a number of critical functions in the system and found additional instances of inappropriate access. Taxation has taken steps to address these instances of inappropriate access since the report was issued in May 2015.

In addition to the actions above, Taxation is in the process of implementing a new access management system and reevaluating its current access structure. Both of these are significant efforts that will take several years to implement. Taxation anticipates the new access management system will provide functionality to allow for automatic and ongoing reconciliation of documented and actual access.

As discussed in our prior report, Taxation has a number of internal controls in place that help mitigate the risks of weaknesses in access controls. We did not find instances where the weaknesses

in access controls resulted in unauthorized transactions in the fiscal year under audit. Taxation plans to address these system access issues in the new access management system to prevent unnecessary risk and noncompliance with Security Standard requirements.

Taxation should continue with its efforts to strengthen access controls over Advantage Revenue. Some of the critical considerations as Taxation moves forward in reevaluating its access structure and implementing a new access management system include:

- Taxation should continue to provide users with accurate, understandable documentation of the access structure to ensure they are able to make well-informed decisions during Taxation's annual access recertification.
- The current user access should be recertified and reconciled to ensure the new access management system is populated with accurate access information.
- Taxation should identify access combinations that create a segregation of duties conflict when evaluating its access structure and ensure effective compensating controls are in place to mitigate the risks associated with them.

Complete System Security Plans

Taxation does not have System Security Plans for its IT resources that meet the requirements in the Security Standard.

Taxation recently developed a System Security Plan template to aid in documenting the security requirements of each IT resource and is now about to begin using these templates to document the requirements. The System Security Plans, when completed, will serve as a central repository of system documentation, including details about the system, risk assessments, specific security configurations, backup and restoration procedures, and vulnerability management. The Security Standard provides guidance on the requirements for sufficient system documentation in sections CM-2, CM-6, and CM-9.

Without System Security Plans, Taxation may not be able to restore critical systems in a timely manner that is consistent with continuity planning and disaster recovery requirements. Additionally, Taxation may not be able to ensure that IT resources are configured according to the requirements of the Security Standard and best practices. This could result in prolonged system unavailability.

Taxation has not completed the System Security Plans due to lack of prioritization of available resources. While Taxation completed the System Security Plan template in June 2014, limitations in available staff have prevented Taxation from collecting the information needed to complete the System Security Plans. Taxation has recently acquired new staff and started the documentation collection effort. Prior to the System Security Plan model, Taxation did not follow a consistent model for the collection, review, and modification of critical system documentation.

Taxation should prioritize and allocate the necessary resources to complete a System Security Plan for each required IT system, starting with its mission critical and sensitive systems.

Improve Database Change Management Controls

Taxation does not have a comprehensive process to manage database change requests (DBCRs). A sample of thirty DBCRs found the following:

- Ten percent of the DBCRs were created and approved by the same user
- Ten percent of the DBCRs were modified by the database administrator prior to implementation

Additionally, Taxation does not maintain clear documentation that the DBCR was tested prior to submission.

The Security Standard, Section CM-1, requires that agencies establish change management policy and procedures that communicate the "purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance" and "facilitate the implementation of the configuration management policy." The Security Standard, Section CM-3, requires that only reviewed and approved changes are implemented. Additionally, the Security Standard, Section AC-5, requires agencies implement segregation of duties to prevent database administrators modifying software code after its change request approval and users self-approving change requests.

Without documented policy and procedures that include the Security Standard's minimum requirements, Taxation cannot clearly communicate to its staff the role that each staff serves in ensuring that only accurate, properly approved, and tested information is entered into its databases. The lack of a comprehensive and documented change management process also leads to inconsistent implementation.

Taxation should review its database change management process to ensure that it is properly documented and includes the minimum requirements outlined in the Security Standard, Sections CM-1, CM-3, and AC-5. Taxation should also implement a process to ensure that the staff using the database change management process are properly trained and understand the risks of not following the established procedures.

Improve Procedures for myVRS Navigator Reconciliations and Data Discrepancies

Taxation is not properly reconciling data discrepancies between the *my*VRS Navigator system and its human resources and payroll systems in a timely manner. Taxation does not have formal written reconciliation policies and procedures, and as a result, Taxation did not investigate any of the 38 discrepancies totaling $3,492 from the February 2015 reconciliation. The reconciliation contained exceptions which date back to October 2012, but had not been investigated or resolved.

With the implementation of *my*VRS Navigator, agencies are responsible for ensuring that all employee data in their payroll and human resource systems is accurately entered into *my*VRS Navigator. The Department of Accounts Payroll Bulletin 2013_02 and the June 2015 Commonwealth Accounting Policies and Procedures (CAPP) Manual, Topic 50410, detail required tasks and roles of agencies in the reconciliation process. The process requires the agencies to play a more significant role in identifying and correcting errors prior to certifying payroll data monthly in *my*VRS Navigator. Not properly reconciling *my*VRS Navigator data with payroll and human resources data increases the risk that Taxation's retirement contributions for its employees will be inaccurate, which could impact retirement benefit payments.

Taxation should establish formal procedures for *my*VRS Navigator reconciliations to ensure that retirement information for all employees is accurate. This should include confirming its payroll, human resources, and *my*VRS Navigator data properly reconcile with one another.

Department of Treasury

Improve Financial Reporting

The Division of Unclaimed Property (Unclaimed Property) did not properly prepare the template submitted to Accounts to accurately reflect the activity of the Unclaimed Property Private Purpose Trust Fund (Fund) for presentation in the Commonwealth's Comprehensive Annual Financial Report (CAFR). Furthermore, Unclaimed Property does not have sufficient documented policies and procedures regarding the preparation and review of the template in accordance with Governmental Accounting Standards Board accounting standards (GASB).

Unclaimed Property's unaudited template for the CAFR's compilation of unclaimed property funds contained misstatements in the detailed securities activity and valuation amounts. Unclaimed Property did not report in the template the activity for securities remitted to and claimed from the custodian. As a result, Unclaimed Property had to make a $22 million adjustment to reflect the details of this activity. Additionally, in reporting the year-end valuation of the securities held, Unclaimed Property used an incorrect securities valuation field from a report provided by the custodian, resulting in a $13 million error.

Sufficiently detailed and documented policies and procedures governing key processes are necessary to maintain adequate internal control over financial reporting and to ensure processes are performed correctly and consistently. The lack of sufficiently detailed and documented policies and procedures presents unnecessary risks in the preparation and review of financial activity, especially when there has been a rotation of Unclaimed Property staff responsibilities or turnover.

Unclaimed Property should develop, document, and follow policies and procedures governing the preparation and review of the template provided to Accounts to ensure they are reporting activity in accordance with GASB standards. Further, Unclaimed Property should evaluate who is responsible for preparing the template and ensure that employee is adequately trained and has the resources necessary to prepare the template accurately. Also, Unclaimed Property should increase communication with Accounts to ensure they understand the nature of the information that should be reported on the template and with the custodian to ensure they are receiving and understand the necessary information in order to accurately complete the template. Finally, a new GASB standard related to fiduciary funds is scheduled to be issued in the near future and may impact the Fund's current financial statement presentation. Unclaimed Property should meet with Accounts to determine how to address these new requirements and update its policies and procedures accordingly.

Improve Change Management Process and Controls

Treasury needs to improve its IT change management program to ensure it meets the minimum requirements in the Security Standard. Specifically, we identified the following weaknesses:

- Treasury's change management process allows the IT developer who creates and modifies application source code to migrate the related code from development and testing environments into the system's production environment. The ability to alter and migrate system code across multiple environments is a violation of separation of duties, as defined in Section AC-5 of the Security Standard. The Security Standard, Section CM-5, further requires that an organization define, document, and enforce access restrictions associated with any information system changes. Also, the Security Standard, Section AC-6, requires that the organization only allow users access to information systems based on the assigned tasks. Allowing developers to modify and migrate code into production system environments increases the risk that system changes will not be approved in accordance with the established Treasury change control policies and procedures and thus circumvent the established control mechanisms. This increases the risk of introducing potential system bugs and vulnerabilities, which could in turn result in system unavailability or compromise. Upon identification of this weakness, Treasury has discontinued its practice of allowing IT developers who created or modified the source code from migrating the code into production; however, this weakness was present throughout the fiscal year in review.

- Treasury does not have a detailed written procedure that clearly defines which changes require a security impact analysis or involve the Information Security Officer in the change management process to ensure the integrity of existing security controls. Additionally, Treasury is using a legacy system, Workspaces, to manage its change control process across multiple mission critical applications. The outdated application increases the difficulty of effectively monitoring and managing the change control process. The Security Standard, Section CM-3, requires that an agency implement change control processes in a way that does not compromise security controls. Also, the Security Standard, Section CM-4, requires that the organization analyze changes to discover potential security impacts before implementation. The Security Standard, Section CM-3, also states that for sensitive systems, the organization is required to have an information security representative provide expertise throughout the change management process. Without sufficient and clear documented guidance, Treasury increases its risk of implementing changes into a production environment that have not been sufficiently tested, approved, and evaluated for potential impacts to security controls. Upon identification of this weakness, Treasury has begun to work on establishing a more robust change management procedure.

Treasury allowed IT developers who created and modified application source code to migrate the related code from development and testing environments into the system's production environment primarily due to limited information technology staffing resources. Treasury does not have a written procedure that defines which changes require a security impact analysis or involve the Information Security Officer primarily due to management oversight.

Treasury should continue to dedicate the necessary resources to improve its change management program to ensure consistent implementation and application of defined change control procedures and provide improved oversight for the changes to Treasury's IT systems. Treasury should also ensure that its change management program aligns with the requirements of the Security Standard. Additionally, Treasury should dedicate the necessary resources to evaluate its current change control application in order to determine if the system is reasonably meeting the agency's needs for enterprise change management.

Improve and Follow Internal Controls for Risk Management Claims Processing

The Department of the Treasury's Division of Risk Management should improve and follow its internal controls to ensure that all claims are processed in a consistent manner and that there is sufficient documentation supporting the validity of each claim. Though Treasury does currently have documentation concerning the processing of claims, the documentation is more focused on individual job responsibilities and not the overall control environment that is in place. While we understand the nature of the work they perform may not lend itself to having detailed steps that cover all aspects of the claims management process, having documented policies and procedures will help ensure that all claims are handled in a consistent and appropriate manner.

During our audit, we found that the Director of Risk Management (Director) did not perform due diligence prior to paying two claims totaling approximately $1,950 over multiple fiscal years from the tort liability program for a member of Treasury's management. The claims were for damage that occurred to the individual's personal vehicle while on official business. For the damage to be covered under the Commonwealth's tort liability program, due diligence should be performed to determine whether an entity or employee of the Commonwealth was responsible for the damage. However, for these two claims, this process did not occur.

The Director is not familiar with the process that is typically followed when reviewing these types of claims, and therefore, these claims did not undergo the same level of review and documentation as claims of a similar nature. We did not find evidence indicating the reason that due diligence was not performed was the result of collusion or the intent to defraud the program. Had a more formal process been in place for processing claims, the Director could have relied on this process to support requesting additional information to validate the claims.

The State Treasurer should work with the Risk Management Division to ensure there are adequate policies and procedures in place to ensure there is sufficient support obtained to show that all factors were considered when evaluating each claim. For any transactions or situations in which the normal process is not appropriate, additional documentation should be retained to provide details on the nature, requirements, and management decision regarding the transaction. In addition, the State Treasurer should re-emphasize within the agency the importance of having and following internal controls in all situations. We also recommend these two claims undergo additional review, and if it is determined that the payments should not have been made, the individual should return the amount to the Commonwealth.

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, 2015, 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 Summer 2016.

- 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 Spring 2016.

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.

Summary of Budget and Expenses for Fiscal Year 2015

Table 1

	Original Budget	Final Budget	Expenses
Secretary of Finance	$ 453,132	$ 619,660	$ 563,389
Department of Accounts	36,765,947	56,109,861	48,645,770
Department of Planning and Budget	7,482,224	7,024,635	5,875,007
Department of Taxation	105,355,128	104,786,347	100,711,019
Department of the Treasury	18,902,642	21,599,546	21,263,138
Total – Finance Agencies	**$168,959,073**	**$190,140,049**	**$177,058,323**

Source: Commonwealth Accounting and Reporting System

The most significant budgetary changes within the Finance agencies took place in Accounts. Instead of sum sufficient adjustments processed throughout the year, internal service funds financed from charges to agencies for the use of Cardinal, the Performance Budgeting System, and Time, Attendance, and Leave were established at the beginning of the fiscal year.

The majority of expenses in the Finance Secretariat are for personal services (approximately 52 percent) and contractual services (approximately 43 percent). Table 2 summarizes the type of expenses each of the Finance Secretariat agencies incurred during fiscal year 2015.

Summary of Expenses by Type for Fiscal Year 2015

Table 2

	Secretary of Finance	Accounts	Planning and Budget	Taxation	Treasury
Personal services	$ 531,939	$13,793,561	$5,094,954	$63,318,960	$ 9,220,001
Contractual services	6,044	33,512,896	409,500	32,060,892	10,823,139
Supplies and materials	427	56,704	21,065	274,550	224,026
Transfer payments		1,235	516	87,454	57,851
Continuous charges	24,979	1,176,251	334,752	4,023,935	884,938
Equipment		103,713	14,220	945,228	53,183
Other	-	1,410	-	-	-
Total expenses	**$563,389**	**$48,645,770**	**$5,875,007**	**$100,711,019**	**$21,263,138**

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 review covers retail sales and use tax with a focus on the collection and distribution of local sales and use taxes. As part of our initial 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 2015, Taxation collected approximately $5.7 billion in retail sales and use taxes, with $1.1 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.

Error Rate for Local Sales Tax Distributions

Table 3

	2013	2014	2015
Local distribution amount	$1,089,743,109	$1,094,793,721	$1,143,329,727
Errors identified and corrected	5,640,689	5,067,477	11,255,590
Error rate	0.52%	0.46%	0.98%

Source: Taxation's Integrated Revenue Management System

As shown above, the error rate for fiscal year 2015 was .98 percent. While this is within the one percent benchmark established in our earlier review, the error rate more than doubled from the previous year. In fiscal year 2015, there was a large increase in transfers attributable to audit refunds compared to the prior fiscal years. This occurs when taxpayers do not allocate the proper amounts to the locality, or a taxpayer has a liability in more than one locality. Based on these results, it appears that the error rate is within the established benchmark, and Taxation is properly distributing the local portion of the retail sales and use tax. We do not recommend any changes in the established benchmark.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

January 26, 2016

The Honorable Terence R. McAuliffe
Governor of Virginia

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

We have audited the financial records and operations of the agencies under the **Secretary of Finance** for the year ended June 30, 2015. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Objectives

Our primary audit objectives for the audit of the Departments of Accounts, Planning and Budget, Taxation, and Treasury for the fiscal year ended June 30, 2015, 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, Cardinal, 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 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*
Commonwealth Accounting and Reporting System (CARS)
Cardinal
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*
Bond Issuance
Debt Service Expenses
Investment Trading
Investment Accounting
Investment Accounting System
Securities Lending Transactions
Bank Reconciliation System
Trust Accounting
Check Processing System
Risk Management Claim System
Unclaimed Property Management System
Administrative Activities

*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, Taxation, and Treasury 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 Cardinal System Security Controls," "Continue to Improve Payline Security," "Continue to Improve Risk Management and Continuity Planning Documentation," "Continue to Improve IT Security Audit Plan," "Update Contingency Planning Documentation," "Improve Administrative Access Controls," "Continue to Strengthen Controls over Advantage Revenue Access," "Complete System Security Plans," "Improve Database Change Management Controls," "Improve Procedures for *my*VRS Navigator Reconciliations and Data Discrepancies," "Improve Financial Reporting," and "Improve Change Management Process and Controls" in the section entitled "Internal Control and Compliance Findings and Recommendations."

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

DLR/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 because 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 2015, over 6,700 administrative adjustments were processed by Planning and Budget resulting in a $2.5 billion increase to the Commonwealth's operating budget. 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 2015, Taxation collected $17 billion in net revenue, depositing $16.5 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 2015, Tax distributed $419.6 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

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 externally managed 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 audits 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, 2014, and reported our audit results in a separate audit report issued in February 2015. Our audits for these entities for fiscal year 2015 will be available later this winter.

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. Cardinal, an enterprise-wide financial system, that Accounts also operates and maintains, will replace CARS beginning in fiscal year 2017. CARS remains the system of record until June 30, 2016. 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, Cardinal, 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 2015.

Sales and use tax for education	$1,270,297,235
Personal Property Tax Relief Act	950,000,000
Recordation taxes	18,302,524
Other	5,415,715
Total	**$2,244,015,474**

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 $19,162,451and $983,112, 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 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 and Cardinal 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

January 29, 2016

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 *Internal Control and Compliance Findings and Recommendations* contained in your 2015 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.

Internal Control and Compliance Findings and Recommendations

Improve Cardinal System Security Controls

From the inception of the Cardinal initiative, Accounts and the Department of Transportation partnered in the planning, design and implementation of the Cardinal System. Between 2011 and 2014, there have been three successful implementations of the system at nearly half of the Commonwealth's agencies. As Accounts prepares for the final implementation of the Cardinal base financial system to the remaining agencies (February 2016), the agency has also made great strides during Fiscal Year 2016 to fully transition all components of the system ownership and the management of the application to Accounts (excluding components managed by Northrop Grumman (NG) under the Commonwealth's Information Technology (IT) Partnership agreement).

While there has been much activity related to the Cardinal implementations and the transition noted above, Accounts and the Cardinal support team understand the importance of ensuring adequate controls, particularly in the area of system security. There has always been a high focus level placed on the system security by the agency and the team. Accounts is committed to implementing the security control improvements recommended in this report.

Continue to Improve Payline Security

Accounts is committed to implementing the security control improvements recommended in this report.

(804) 225-2109 FAX (804) 786-3356 TDD (804) 371-8588

Continue to 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. Accounts has participated in Disaster Recovery planning and execution annually including 2015. The COOP plan has been updated as of April 2013 and will be undergoing another update incorporating the business changes associated with Cardinal. Although not complete, Accounts will dedicate the necessary resources to complete the agency's Business Impact Analysis and Risk Assessment plans.

Continue to 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 documentation as well as incorporate the findings into the required three year audit plan for sensitive systems. Accounts will finalize the contract with an outside auditing firm to conduct IT security audits of the agency's sensitive systems.

Sincerely,

David A. Von Moll

Copy: The Honorable Richard D. Brown, Secretary of Finance
Lewis R. McCabe, Jr., Deputy State Comptroller

COMMONWEALTH of VIRGINIA
Department of Planning and Budget

DANIEL S. TIMBERLAKE
Director

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

January 29, 2016

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

Dear Ms. Mavredes:

The Department of Planning and Budget (DPB) has reviewed the findings and recommendations provided by the Auditor of Public Accounts as part of your audit of financial records and operations for the fiscal year that ended on June 30, 2015. I offer the following response to your team's internal control and compliance finding and recommendation for DPB.

Update Contingency Planning Documentation

I appreciate the auditor's acknowledgement of DPB's actions to procure the services of the Virginia Information Technologies Agency's Small Agency Information Security Office (ISO) program, an action based on a prior management recommendation. With the assistance and advice from staff of the ISO program, DPB took corrective action in December of 2015 to ensure that its Mission Essential Functions (MEFs), as identified in the Continuity of Operations Plan (COOP) and Disaster Recovery Plan (DRP), are consistent with and align to DPB's Business Impact Analysis.

Thank you again for the opportunity to respond to your report.

Sincerely,

Daniel S. Timberlake

c: The Honorable Richard D. Brown

FAX (804) 225-3291 (804) 786-7455 TDD (804) 786-7578

COMMONWEALTH of VIRGINIA

Department of Taxation

January 11, 2016

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

Dear Ms. Mavredes:

Below are Department of Taxations' (TAX) responses to the audit for the Fiscal year ended June 30, 2015. I and my staff appreciate the diligence, abilities, and professionalism of your staff in the performance of the audit of an agency as complex as TAX.

TAX places great emphasis on it responsibility to protect the confidentiality, integrity and availability of taxpayer information. Although there are four comments which describe the need for enhancements in TAX's technology controls, there are compensating system safeguards that exist which are not described in the report which mitigate any residual risks. In fact, one of the comments explicitly notes that there were no instances where weakness in access controls resulted in unauthorized transactions. I also note that two recommendations relate to essentially the same subject, one dealing with improving Administrative Access Controls and the other dealing with access controls for a specific application (Advantage Revenue). The recommendations are so interrelated they have the same response. Although I think it is appropriate to question the significance of some of the issues noted, I nonetheless expect TAX to implement corrective actions to address your findings that include the following:

Improve Administrative Access Controls

In response to this management recommendation, TAX will implement an identity management application. Although the timeline for full implementation of this application extends to 2017, TAX will implement this application sufficiently by September 30, 2016 to address the issues noted in this recommendation.

Continue to Strengthen Controls over Advantage Revenue Access-Repeat

Although the comment is a repeat comment TAX has completed all the actions that could be taken to address the issue except for completing the identity management application implementation. TAX has completed the following actions to address the issues noted in the previous comment:

1) Procured and prototyped a new identity management application(Sailpoint) that will facilitate the management of privileges at the granular level suggested by APA,

2) Revised the process for voucher approvers so that approvers do no edit the same voucher they have approved,

3) Reengineered the process for reviewing large dollar individual refunds so that the ability to approve these transactions could be removed from 136 individuals,

4) Performed an independent review of 1,576 user's access privileges to 27 financial functions within the Advantage Revenue application and removed the access where it was not needed on a regular basis, and;

5) Performed a management review of all user access privileges for all systems and applications managed by the existing identity management application (SAFE).

In response to this management recommendation, TAX will implement an identity management application. Although the timeline for full implementation of this application extends to 2017, TAX will implement this application sufficiently by September 30, 2016 to address the issues noted in this recommendation.

Complete System Security Plans

TAX received funding in the 2015 Appropriation Act for a resource to complete the System Security Plans. Although the staff resource has been hired and work has been completed, there was not sufficient time to complete the System Security Plans before the audit testing. TAX will complete a System Security Plan for each mission critical or sensitive system by September 30, 2016.

Improve Database Change Management Controls

TAX will review its database change management process to ensure that it is properly documented and includes applicable VITA security requirements. Employees will be properly trained on the revised process. These tasks will be completed by September 30, 2016.

Improve Procedures for myVRS Navigator Reconciliations and Data Discrepancies

The comment notes that there were 38 discrepancies between myVRS Navigator system and TAX's human resources and payroll systems as of February 2015. As of December 1, 2015; 32 of the discrepancies have been resolved. One of the discrepancies will be resolved by September 30, 2016 and the remaining five discrepancies will never be resolved. These five

discrepancies all involve deceased employees where TAX was not notified of the discrepancy in a timely enough manner to resolve the discrepancy through the employee's estate. These five discrepancies will be reflected on the reconciliation as a permanent difference.

Risk Alert

I appreciate the acknowledgment that TAX is not responsible for the issues appropriately outlined in the Risk Alert. At the same time, I would like to note the repeated actions TAX has taken to prompt the "Partnership" to take action on the important issues described in the Risk Alert even though TAX is essentially powerless to facilitate resolution of the issues. When the "Partnership" was formed, staff and resources to perform these functions were removed and transferred to the "Partnership." TAX does not retain even the ability to withhold payment for the services your report notes were not provided. TAX can only request issues such as these be addressed and has done so in the past. A recent communication on an issue raised by APA is attached.

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

COMMONWEALTH of VIRGINIA

Department of Taxation

July 28, 2015

Mr. Nelson Moe
Chief Information Officer
Commonwealth of Virginia
11751 Meadowville Lane
Chester, Virginia 23836

Dear ~~Mr. Moe~~ Nelson:

First, I want to congratulate you on recently becoming the Commonwealth's Chief Information Officer. I know the transition to your current position will initially require a great deal of your time gaining familiarity with the state's complex information technology platform and my staff is available to assist in any way you deem appropriate or necessary.

Second, I call to your attention the July 28 email from Sharon Kitchens to your staff regarding the past weekend's efforts by Northrop Grumman (NG) to apply patches to Taxation's servers. While I admit I do not have the technical background to understand why patching is routinely required, it appears to me that properly and timely applied patches are what I would call a tip of the spear in protecting the sensitive electronic data processed and stored in our network.

Respondents (citizens, practitioners, and businesses) to our recent strategic planning process clearly articulated an expectation that their personal data entrusted to the Department of Taxation be kept secure and confidential. By not properly and timely applying patches data security is at greater risk and negates the diligence and effort with which Taxation's technology team works through other means to properly protect this data.

I would appreciate your perspective on the issues raised by Ms. Kitchens and what steps will be taken by NG to bring this basic, yet critical, measure into compliance. Feel free to contact me at 786-3332 with any questions or concerns.

Sincerely,

Craig M. Burns
Tax Commissioner

COMMONWEALTH of VIRGINIA
Department of the Treasury

MANJU S. GANERIWALA
TREASURER OF VIRGINIA

P.O. BOX 1879
RICHMOND, VIRGINIA 23218-1879
(804) 225-2142
FAX (804) 225-3187

February 17, 2016

Ms. Martha Mavredes
Auditor of Public Accounts
101 N. 14th Street, 8th Floor
Richmond, VA 23219

Dear Ms. Mavredes,

The Department of the Treasury (Treasury) appreciates the opportunity to respond to both the *Improve Financial Reporting* and the *Improve Change Management Process and Controls* recommendations in your Report on Audit of the Agencies of the Secretary of Finance for the fiscal year ended June 30, 2015. Your comments and recommendations are appreciated and given the highest level of consideration by Treasury as we continually strive to improve our processes.

Comments to Management

Improve Financial Reporting

Unclaimed Property management has already reached out to the Department of Accounts to discuss the expected new GASB standard related to fiduciary funds. Staff is also in the process of drafting procedures for completing the financial statement template and related processes. Additionally, Unclaimed Property will work with the custodian to receive more detailed reports to aid in the financial reporting process.

Improve Change Management Process and Controls

As noted in your report, Treasury has already discontinued its practice of allowing IT developers who created or modified the source code from migrating the code into production. Additionally, Treasury will complete its work on a more robust, written change management procedure.

Improve and Follow Internal Controls for Risk Management Claims Processing

Treasury will review its policies and procedures for Risk Management's claims processes with staff and will strengthen, as necessary. Additionally, another staff member in the Risk Management Division will perform a secondary review of the claims in question to validate them.

Sincerely,

Manju S. Ganeriwala

cc: The Honorable Ric Brown, Secretary of Finance

SECRETARY OF FINANCE AGENCY OFFICIALS

As of June 30, 2015

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