AGENCIES OF THE SECRETARY OF TRANSPORTATION

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

Report Highlights

Audit of the Agencies of the Secretary of Transportation – For the Year Ending June 30, 2015

Martha S. Mavredes, CPA

January 2016

Summary of Audit Results

During our audit, we found the following:

- Proper recording and reporting of transactions, in all material respects, in the Commonwealth Accounting and Reporting System and in each agency's accounting records;
- One matter that we consider to be a **material weakness** in internal controls;
- Nineteen additional matters that we consider to be **significant deficiencies** in internal control; and
- Instances of noncompliance with applicable laws and regulations that is required to be reported under Government Auditing Standards.

Summary of Selected Issues and Recommendations

[1] finding related to the internal controls surrounding the financial reporting process which we consider to be a material weakness. The **Virginia Department of Transportation (Transportation)** should enhance their reviews of financial information provided to the Department of Accounts for inclusion into the state's Comprehensive Annual Financial Report.

[1] risk alert related to the Commonwealth of Virginia's information technology infrastructure and its reliance upon **the Virginia Information Technology-Northrop Grumman Partnership (Partnership).** The Partnership is responsible for maintaining and administering more than 100 server operating systems for Transportation and more than 130 server operation systems for Motor Vehicles that their respective vendors have ceased supporting. The Commonwealth should ensure that the Partnership upgrades these end-of-life systems to decrease vulnerabilities caused by unpatched and unsupported systems.

[12] findings related to the General Controls around **Information Systems.** These findings are related to information system management not ensuring compliance to the **Commonwealth Security Standard**. These findings should be of concern to the **Virginia Information Technologies Agency (VITA) and the Department of Accounts,** as they are responsible for issuing guidance in these areas. Many of the affected systems provide financial information that is reported in the Commonwealth's CAFR issued by the **Comptroller.**

[7] findings related to internal controls and compliance with **Internal and Commonwealth Policies and Procedures.** These findings cite **specific exceptions** with the applicable policies and procedures and prove recommendations for remediation to reduce risk. These issues may require additional resources and supervision in order to correct; and therefore, should be monitored by management.

Why the APA Audits These Two Agencies Every Year

Collectively the following two agencies spent $5.2 billion, or 92%, of the total funds expended by the **Agencies under the Secretary of Transportation**:

- **Department of Transportation;**
- **Department of Motor Vehicles**

As a result, these two agencies are material to the **Comprehensive Annual Financial Report (CAFR)** of the Commonwealth. Therefore, we are required to audit their financial activities in support of our audit opinion on the CAFR. Additionally, the federal government required us to audit one federally supported program for compliance in fiscal year 2015. We reviewed the controls and audited compliance for this program in support of the **Commonwealth's Single Audit**.

–TABLE OF CONTENTS–

Why the APA Audits the Departments of Transportation and Motor Vehicles

Collectively, the Departments of Transportation and Motor Vehicles spent $5.2 billion, or 92%, of the total funds expended by the agencies under the Secretary of Transportation during state fiscal year 2015. As a result, these two agencies are material to the Comprehensive Annual Financial Report (CAFR) of the Commonwealth. Therefore, we are required to audit their financial activities in support of our audit opinion on the CAFR. Our audit of the 2015 financial activity yielded the risk alert and findings below. Appendix A provides details on the sources and uses of funds for all agencies under the Secretary of Transporation.

RISK ALERT

A Risk Alert differs from an Audit 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.

Upgrade or Decommission End-of-Life Server Operating Systems

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 review, 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.

The Partnership uses end-of-life and unsupported server operating systems in its IT environment to support some of the Department of Transportation's (Transportation) and Department of Motor Vehicles' (Motor Vehicles) mission-critical functions. Transportation and Motor Vehicles rely on the Partnership to provide current, supported, and updated server operating 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 more than 90 server operating systems for Transportation, and more than 130 server operating systems for Motor Vehicles that the respective vendor designates as end-of-life. The Partnership's use of unsupported server operating systems increases the risk that existing vulnerabilities will persist in the server operating 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 server operating systems designated as end-of-life, which increases the difficulty of restoring system functionality if a technical failure occurs.

Transportation and Motor Vehicles are aware of this issue and are working with the Partnership to develop remediation plans during 2016 to upgrade, decommission, or request exceptions for the end-of-life server operating systems. Until then, Transportation, Motor Vehicles, 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 environments.

The Partnership should continue working with Transportation and Motor Vehicles to upgrade or decommission all of the end-of life server operating systems as soon as possible. Doing this will further reduce the risk to the confidentiality, integrity, and availability of sensitive Commonwealth data and achieve compliance with the Security Standard.

AUDIT FINDINGS AND RECOMMENDATIONS

Department of Transportation

Why the APA Audits Financial Reporting

Transportation spends nearly $5 billion annually in order to support and maintain Virginia's roadway infrastructure. Transportation is thus individually material to the CAFR. We have audited the accuracy of information within Transportation's financial reporting as well as the internal controls that surround these processes. Our testwork resulted in the following two recommendations to management.

Improve Controls over Financial Reporting
Repeat Finding, Material Weakness

Transportation does not have adequate internal controls over its financial reporting processes. In the past two years, Transportation has made errors in its unaudited financial submissions to the Department of Accounts (Accounts). This year, we again identified significant misstatements in Transportation's disclosure for contractual commitments, unaudited accounts receivable, net investment in capital assets, and other disclosures. These misstatements resulted in aggregate audit adjustments of over $150 million, the majority of which related to disclosures. As a result, we consider this matter to be a material weakness in internal control.

All submissions are to be submitted by established due dates and contain complete and accurate information, according to Accounts' Financial Reporting Directive 4-15 from the Office of the Commonwealth's Comptroller. Transportation has over 60 submissions to prepare and send to Accounts each year within a short window of time. The majority of these submissions are without error, but some have continued to contain errors each year.

The quality of Transportation's review of these submissions contributed to these errors. In addition, there is no independent reviewer with knowledge of all operations and accounting, reviewing each submission for accuracy.

The Transportation Controller and the Fiscal Division should ensure their financial reporting procedures over these areas are enforced and that a thorough review process prevents and detects mistakes. The Controller should also ensure that an individual who is independent of the area that prepared each submission review them for accuracy. The Fiscal Division should supplement this by increasing analytical procedures, reviews of variances, and overall reviews of all items to ensure they are reasonable and consistent across submissions. Improved financial reporting controls will help ensure Transportation's unaudited financial submissions are materially correct and accurately represent its operations to meet the Commonwealth's financial reporting needs.

Document Impact Funding has on Highway Infrastructure Capitalization
Significant Deficiency

Transportation does not have documented internal controls to consider the financial reporting implications that changes in funding legislation could have on highway infrastructure capitalization. The General Assembly enacted alternative paving funding legislation in 2013 under Code of Virginia Section 33.2-358(C), which enabled Transportation to fund additional paving rehabilitation projects in the Acquisition and Construction program. Transportation's infrastructure capitalization methodology considers projects funded in this program are capitalizable.

Transportation has an established process to monitor legislation and consider the effects on many aspects of the agency's operations. Although the Chief Financial Officer was involved in drafting and implementing the alternative paving funding legislation; therefore, ensuring that Transportation carried out the legislative intent of the funding, the Controller and Fiscal Division did not document the decision process to determine which projects to fund with the additional funding and any effect on infrastructure capitalization. During fiscal year 2015, Transportation funded over $102 million in projects under this legislation and capitalized the expenses. Our review of these projects determined that all of the projects funded in fiscal year 2015 were properly capitalized.

The Chief Financial Officer, Controller, and Fiscal Division should document internal controls and processes to consider funding legislation and its effect on highway infrastructure capitalization. When new legislation arises, the Controller and Fiscal Division should document considerations and impacts on the infrastructure capitalization methodology. The Fiscal Division should periodically review the highway infrastructure capitalization methodology to ensure that it is still reasonable and applicable based on legislation and operational changes. The Fiscal Division should continue to ensure that any projects funded in the Acquisition and Construction program are capitalizable under the current methodology.

Why the APA Audits Information System Security

Transportation collects, manages, and stores significant volumes of project, transactional, and financial data within its mission critical systems. Because of the highly critical nature of this data, Transportation's management must take all necessary precautions to ensure the availability, integrity, and security of the data within its systems. We compared Transportation's practices to those required by the Commonwealth's Information Security Standard in the areas of database security, web application security, oversight of sensitive systems, and information system access. Our information system security testwork resulted in the following five recommendations to management.

Develop and Implement IT Hardening Procedures
Significant Deficiency

Transportation has not developed formal hardening procedures that establish secure configuration settings for the agency's information systems. Currently, Transportation's Information Technology Division (IT) has an informal systems hardening process but is not implementing security configurations consistently to all applications. We identified and communicated system specific control weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

The Security Standard, section CM-6, requires Transportation to establish and implement configuration settings for information technology products employed within the information system using the Commonwealth of Virginia System Hardening Standards that reflect the most restrictive mode consistent with operational requirements. The Security Standard, Section CM-6, further requires Transportation to identify, document, and approve any deviations from established configuration settings for information system components based on operational requirements. Additionally, the Security Standard, Section CM-6, requires that Transportation monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Establishing hardening procedures better ensures that mission critical systems have appropriate configurations, and serves as a basis for implementing or changing existing information system configurations. Transportation has sensitive systems that perform critical tasks for the citizens of the Commonwealth of Virginia, and by not having formal hardening procedures to apply baseline security configurations, the risk that these systems will not have minimum security requirements to protect data from malicious parties increases.

IT should document and formally approve hardening procedures for their information systems to meet the requirements in the Security Standard. IT should also implement and apply the related security configurations to all systems within its information technology environment. Further, IT should implement the additional controls discussed in the communication marked FOIAE

in accordance with the Security Standard. This will enhance Transportation's risk of attacks from malicious parties.

Improve the Sensitive System Classification Process
Significant Deficiency

Transportation lacks a formal methodology to properly identify and classify its sensitive systems. IT's internal procedures as well as the Security Standard require that systems receiving a ranking of "high" on the criteria of confidentiality, integrity, and/or availability should be classified as sensitive on the agency's sensitive system listing. Currently, IT has ranked several systems as "high" on Transportation's Business Impact Analysis (BIA) for confidentiality, integrity, and availability but those systems are not on the agency's sensitive system listing. Misclassifying a sensitive system as non-sensitive increases the risk it will not have the necessary controls in place to adequately protect the data that it manages, stores, or processes and that these controls will not be regularly evaluated.

IT has limited procedures in place to identify and classify sensitive systems, but is not currently documenting their justification for classifying systems as non-sensitive that receive a "high" rating in the criteria of confidentiality, integrity, and availability. This lack of procedural documentation is resulting in the noted inconsistencies between the agency's sensitive system listing and BIA.

IT should evaluate its methodology for identifying and classifying sensitive systems. IT's methodology should require a documented justification from the Information Security Officer when systems that receive a ranking of "high" in the criteria of confidentiality, integrity, or availability by the data owner are not classified as sensitive in the sensitive system listing. Properly identifying all sensitive systems within the information technology environment will better ensure that the necessary security controls will be applied to protect the confidentiality, integrity, and availability of data within the related deemed sensitive systems and that the proper evaluation of these controls is performed.

Improve Access Controls to IT Hardware
Significant Deficiency

Transportation is not granting access into its server room based on the principle of least privilege. The Central Office server room houses multiple mission-critical and sensitive systems that contain confidential data. Currently, there are 207 employees of Transportation, Virginia Information Technologies Agency, and Northrop Grumman with access into the server room.

The Security Standard, Section AC-6, requires Transportation to allow employees access only when that access is necessary to accomplish assigned tasks in accordance with organizational mission and business functions.

By not adhering to the principle of least privilege, the risk that Transportation may be unable to adequately protect sensitive information technology systems is increased, which may result in the compromise of sensitive Transportation systems and data.

IT has granted excessive access to the Central Office server room primarily due to a technical maintenance event that occurred earlier during the fiscal year. A server went offline in the Central Office server room and there were no Northrop Grumman employees available who had pre-established access. As a result, Northrop Grumman subsequently requested that IT grant computer room access to all individuals potentially requiring access to support Transportation's information technology infrastructure on an ongoing basis.

IT should reduce the list of users with access to the server room to only the individuals that require it. Reducing the number of users with access to the Central Office server room will allow IT to perform more efficient user access reviews and help to protect the confidentiality, integrity, and availability of sensitive Transportation data. IT should also develop and implement periodic monitoring and review controls over physical access to the server room to prevent this issue from reoccurring.

Improve Vulnerability Scanning and Remediation Procedures
Significant Deficiency

Transportation does not perform periodic vulnerability scans on their publicly facing and defined sensitive systems. Transportation also does not periodically review or evaluate reports from certain system vulnerability and baseline scanning tools. Reports from these tools enable system administrators to evaluate and determine if their systems are in line with recommended vendor security settings and industry best practices. We identified and communicated the specific control weakness to management in a separate document marked FOIAE under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

The Security Standard, Sections RA-5 and RA-5-COV, requires Transportation to have established vulnerability scanning procedures and employ vulnerability scanning tools at least once every 90 days for sensitive and public internet facing systems. The Security Standard further requires that Transportation analyze scan reports and results from security control assessments, and remediate legitimate vulnerabilities in a timely manner, or within 90 days.

Using scanning tools provides information on sensitive systems such as missing critical patches, inappropriate permission levels, and inappropriate technical configurations and settings. Organizations should use these results to better enhance and refine the security controls and configurations for sensitive and internet facing systems, thereby reducing security risks. Not having formal procedures to require system owners and administrators to perform periodic vulnerability scans and remediate the noted results on a timely basis increases the risk that malicious users will discover and exploit known vulnerabilities in mission-critical systems and data.

IT should implement a vulnerability scanning policy and procedure to ensure that all system owners and system administrators are required to perform vulnerability scans on publicly facing and defined sensitive systems. This will help to ensure IT remediates reported legitimate vulnerabilities on a timely basis. Additionally, IT should implement the additional controls discussed in the communication marked FOIAE in accordance with the Security Standard.

Upgrade End-of-Life Technology
Significant Deficiency

Transportation does not upgrade certain software components supporting mission-critical and sensitive systems within the information technology environment on a timely basis before they are unsupported by the vendors. IT has a remediation plan in place to upgrade, decommission, or get an exception from the Partnership for the end-of-life technology during 2016, but does not currently have approved security exceptions from the Commonwealth of Virginia's Chief Information Security Officer (CISO) for the associated end-of-life software. We identified and communicated the system and component specific control weaknesses to management in a separate document marked FOIAE under Section 2.2-3705.2 of the Code of Virginia due to it containing specified descriptions of security mechanisms.

The Security Standard, Section 8.17, Sub-section SI-2-COV, requires that organizations prohibit the use of products designated as end-of-life/end-of-support by the vendor or publisher. The Security Standard, Section 1.5, further requires that if an agency determines that compliance with the provisions of the Security Standard or any related information security standards adversely affects a business process of the agency, the Agency Head may request approval to deviate from a specific requirement by submitting an exception request to the Commonwealth of Virginia's CISO.

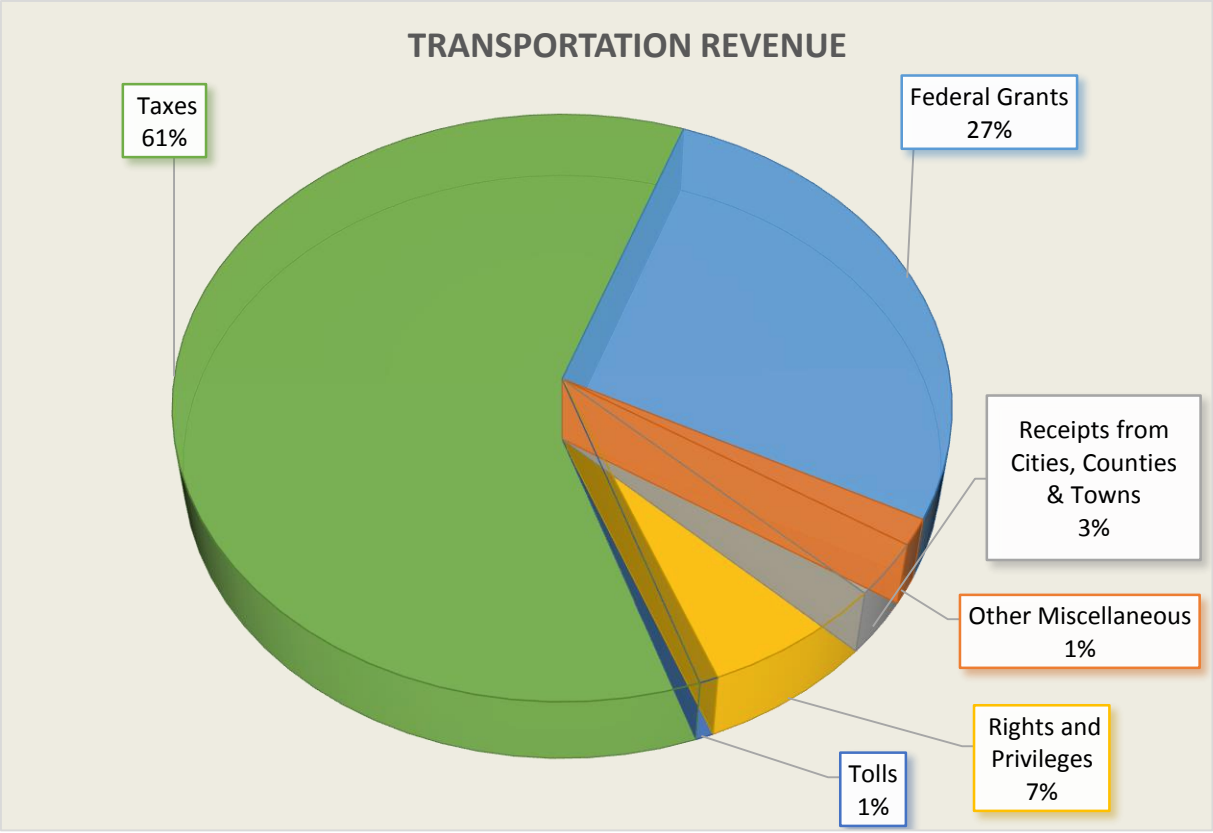
By using unsupported technology, IT can no longer receive and apply security patches for known vulnerabilities, which increases the risk that a malicious attacker will exploit these vulnerabilities leading to a data breach. Additionally, vendors do not offer operational and technical support for end-of-life/end-of-support technology, which effects data availability by increasing the difficulty of restoring system functionality if a technical failure occurs.

IT should prioritize the upgrade and decommissioning of all end-of-life/end-of-support technology discussed in the communication marked FOIA-Exempt in accordance with the Security Standard. IT should also submit security exceptions to the Commonwealth of Virginia's CISO for approval to continue operating the end-of-life technology as necessary. Further, IT should ensure there are sufficient resources in place to complete their remediation plan during 2016. This will better ensure the confidentiality, integrity, and availability of sensitive Commonwealth data and achieve compliance with the Security Standard.

Why the APA Audits the Highway Planning and Construction Grant

The Highway Planning and Construction Grant for construction and some maintenance of the Commonwealth's roadways represents approximately $1.3 billion in annual federal expenditures that support improvements to the Commonwealth's infrastructure. Transportation is the Commonwealth's administrator of this program and is responsible for ensuring compliance with all federal regulations. Federal grant revenue is vital to Transportation's operations as it makes up 27 percent of Transportation's revenues.

We compared various aspects of the Highway Planning and Construction Program to federal regulations in the areas of allowable costs, time and effort reporting, procurement standards, monitoring, and reporting. We also evaluated Transportation's internal controls to ensure compliance to federal regulations pertaining to this program.



Improve the Billing Process
Significant Deficiency

Transportation is not submitting all bills for reimbursement in a timely manner. During our review, we found the following:

- Transportation billed over $20 million for reimbursement from the Federal Highway Administration's Eastern Federal Lands Division (EFL) in excess of six months after incurring the expenses for two projects. Of these billings, $16 million were delayed up to ten months after the expenses. Transportation had no documented procedures in place for manually processing invoices to EFL and there was no backup person in place to perform this when the person responsible for billing was absent.

- Transportation accrued over $4 million in receivables from Motor Vehicles, which it did not bill for over two months after becoming receivable. This caused Motor Vehicles' records to be misstated at year-end.

- Transportation was unable to bill timely for $292,898 in federal reimbursements because it did not adequately monitor the authorization for a federal project and submit a request for additional funds in advance of project expenses.

Commonwealth Accounting Policies and Procedures Manual Topic 20505 states that agencies should have systems in place to bill timely, and accounts should be billed when goods are provided or services rendered. Without requesting federal funds in a timely manner, Transportation relies upon state monies to fund projects, forgoes any interest that could be earned, and may potentially take on fewer projects if federal funds are not immediately available.

Transportation's Fiscal Division should document and implement a method for processing federal bills for all projects outside the normal federal billing process and designate a backup person to perform this function when the primary billing person is absent. The Fiscal Division should also strengthen the monitoring process over all federal projects to ensure funds are available to be invoiced, and ensure federal-aid Project Agreements are updated when the estimated project costs exceed the authorized amount. This will increase access to funds and decrease the risk of bills not being sent.

Improve the Process of Disclosing Economic Interests
Significant Deficiency

Transportation is not properly identifying employees in positions of trust and requiring them to disclose potential conflicts of interest. During our review, we found that Transportation's Human Resources Division did not require employees involved in the procurement of external contracts or those supervising these processes to file Statement of Economic Interest forms. In addition, for one position identified as a position of trust, Transportation did not require the filing of the proper form as a new person assumed this role.

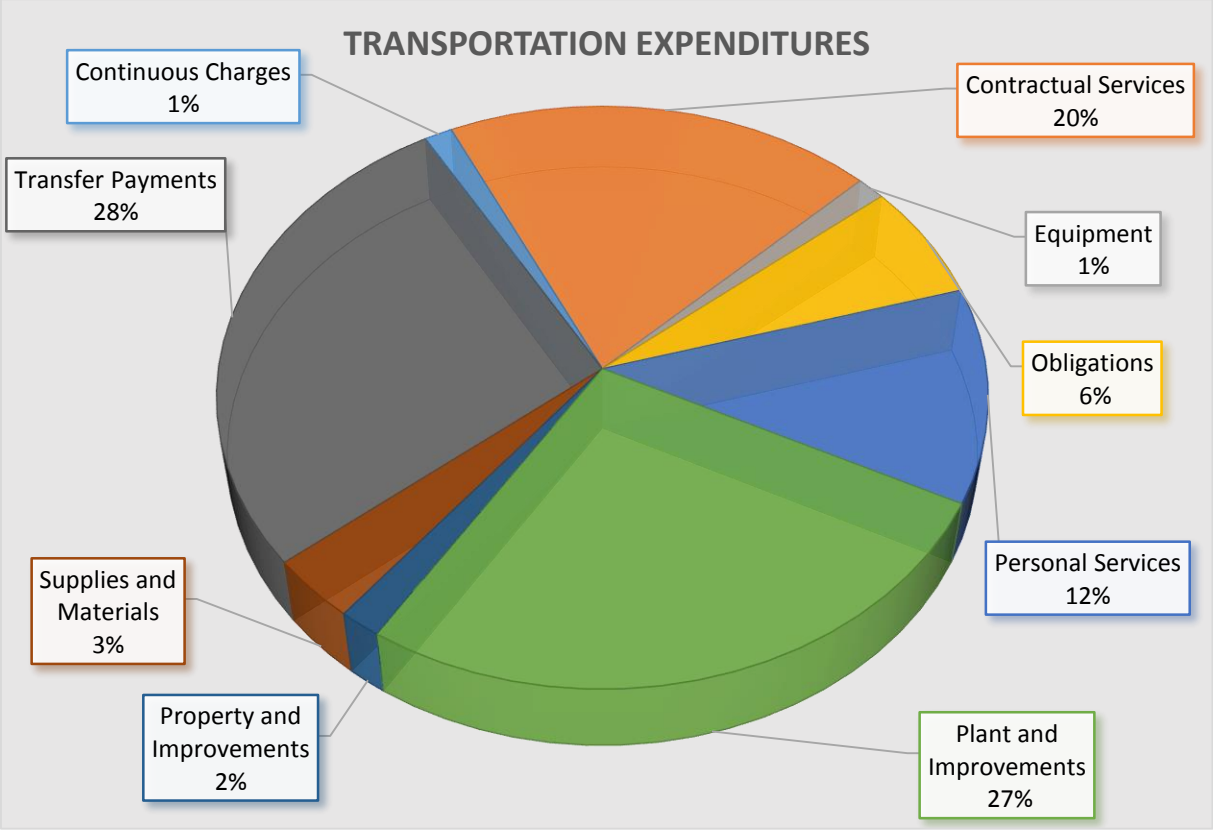
Section 2.2-3114 of the Code of Virginia outlines the principles by which state agencies identify employees in positions of trust and requires them to file Statements of Economic Interest. Further, Executive Order 33 issued by the Office of the Governor clarifies that those in senior-level positions and those with responsibility for substantive authorization and decision-making regarding contracts and procurement are included in this group.

By not properly identifying individuals in positions of trust and having them disclose their economic interests, Transportation could create a potential conflict in the decision making process and a lack of transparency. This could permit the willful misuse of the Commonwealth's funds for the betterment of an individual with an undisclosed economic interest.

Human Resources should create and implement policies and procedures over the Statement of Economic Interest process that properly identify employees in positions of trust, and address employees' movements within the organization. Human Resources should require these individuals to disclose their economic interests and file the proper form with the Secretary of Administration as outlined in the Code.

Why the APA Audits Payroll and Human Resources

Transportation spends over $580 million, or 12 percent of its budget, on payroll and other personal service expenses. Due to the significance of this activity, we consider payroll and human resource controls to be critical. These controls ensure both the accuracy of payroll and compliance with state payroll requirements. We evaluated Transportation's practices against their own policies as well as the requirements set by Department of Accounts and Department of Human Resource Management. Our testwork resulted in the following two management recommendations.



Improve Access Controls to Information Systems
Significant Deficiency

Transportation is not properly removing terminated employees' access to information systems in a timely manner. The Security Standard instructs agencies to promptly remove access when the access is no longer required.

During our review, we found three employees with access to the payroll system whose access was not removed up to three months beyond their termination dates and one employee still had

access at the time of our review. This was due to supervisors not promptly reporting terminations to information security personnel.

Terminated employees with access to information systems increases the risk of alterations of data and/or inappropriate transactions. Transportation supervisors should notify system administrators of terminated users immediately or in advance of termination, and perform automated reviews of access to the payroll system. This will decrease the risk of improper transactions taking place.

Improve the Reconciliation to the Retirement System
Significant Deficiency

Transportation does not adequately reconcile the Commonwealth Integrated Personnel and Payroll System (CIPPS), Personnel Management Information System, and the Virginia Retirement System's (VRS) *my*VRS Navigator System on a regular basis. During our review, we noted instances of discrepancies between the three systems that were not resolved for several months.

The Department of Accounts, in Payroll Bulletin 2013-02, requires agencies to identify and correct errors prior to certifying payroll information in *my*VRS Navigator on a monthly basis. Additionally, Commonwealth Accounting Policies and Procedures Manual Topic 50410 requires each agency to reconcile VRS contributions to CIPPS monthly.

Without proper reconciliation, there is no way to know that information in *my*VRS Navigator is accurate. This can lead to errors in employees' records, which can cause employees who retire to have an incorrect amount of retirement contributions, and/or cause misstatement in VRS' records.

Human Resources should perform a more detailed reconciliation, document the process in more detail, and review and resolve errors on exception reports on a monthly basis. This will reduce the risk of incorrect information being reported to VRS.

Department of Motor Vehicles

Why the APA Audits Information System Security

Motor Vehicles collects, manages, and stores significant volumes of financial and personal data within its mission critical systems. Because of the highly critical nature of this data, Motor Vehicle's management must take all necessary precautions to ensure the availability, integrity, and security of the data within its systems. We compared Motor Vehicle's practices to those required by the Commonwealth Information Security Standard in the areas of database security, web application security, oversight of sensitive systems, and information system access. Subsequently, our information system security testwork resulted in the following six recommendations to management.

Continue to Improve Database and Application Baseline Security Configurations
Repeat Finding, Significant Deficiency

Motor Vehicles continues to not have sufficient security controls in place to adequately protect two of its mission critical and sensitive systems. These weaknesses are due to a continued lack of documented and implemented application and database baseline security configurations. Since the prior review, Motor vehicles has reasonably developed policies and procedures to better ensure that all sensitive and mission critical systems will have developed baseline configurations in the future. The related policies and procedures have not been implemented to date, but are a component of a significant security and information technology operations remediation project, known as the Security Blitz. The Security Blitz project is a major undertaking involving collaboration among an outside vendor, and several internal departments and organizational units within Motor Vehicles.

Our review noted an area of weakness for each system, which we have communicated in detail to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under Section 2.2-3705.2 of the Code of Virginia, due to their sensitivity and description of security controls. We recommend that Motor Vehicles Information Technology Division implement the controls discussed in our recommendation in accordance with the Security Standard.

Continue to Improve Physical and Environmental Security Controls
Repeat Finding, Significant Deficiency

Motor Vehicles continues to not have adequate physical and environmental security controls in place to protect its information technology systems that house sensitive data. These weaknesses continue to exist because Motor Vehicles is currently in the process of consolidating multiple sever rooms in it's headquarter facilities into a single newly constructed data center that can be better managed and more adequately controlled.

Our review noted several areas of weakness that we have communicated in detail to management in a separate document marked FOIAE under Section 2.2-3705.2 of the Code of Virginia,

due to their sensitivity and description of security controls. Motor Vehicles should continue to dedicate the necessary resources to implement the controls discussed in our recommendation in accordance with the Security Standard.

Continue to Improve IT Risk and Continuity Management Program
Repeat Finding, Significant Deficiency

Motor Vehicles continues to not consistently and properly manage certain aspects of their Information Technology (IT) Risk and Continuity Management Program in accordance with the Security Standard. The success of an IT Risk and Continuity Management Program is dependent on the quality and accuracy of key program documents, including IT system risk assessments, business impact analysis, agency and IT continuity of operations plans, and IT disaster recovery plans.

The Security Standard identifies required program documents and elements that should be defined within them. It further lays out specific review and update schedules for these documents, as well as testing expectations for disaster recovery plans. These documents are essential for protecting agency IT systems by identifying risks, vulnerabilities, and remediation techniques; as well as establishing prioritization for restoring systems in contingency and disaster scenarios.

In the prior year we identified several weaknesses with these required documents that have not been addressed. Because of these weaknesses, Motor Vehicles may not be able to effectively and proactively protect sensitive data against risks, vulnerabilities, and threats. This may prevent Motor Vehicles from adequately performing critical business processes in the event of a natural disaster, service disruption, or other occurrence.

The related weaknesses continue to exist because Motor Vehicles has chosen to update its IT Risk and Continuity Management Program and the associated artifacts as a component of a significant security and IT operations remediation project, known as the Security Blitz. The Security Blitz project is a major undertaking involving collaboration among an outside vendor and several internal departments and organizational units within Motor Vehicles.

Motor Vehicles should continue to allocate the necessary resources to review and revise the documents supporting their IT Risk Management and Continuity Management Program to ensure they are consistent and in accordance with the Security Standard. Motor Vehicles should also ensure all components of their IT Disaster Recovery Plan are periodically tested to ensure it can restore all critical systems in the event of a disaster, while also identifying opportunities to improve the disaster recovery process where needed.

Improve IT Software Maintenance and Management Controls
Significant Deficiency

Motor Vehicles does not adequately upgrade some of the IT software that supports critical business processes within the IT environment on a timely basis before they are unsupported by their associated vendor. The related IT software supports systems controlling important agency business functionality, such as remittance processing, fuels tax tracking, and financial analysis. The Security

Standard requires that organizations prohibit the use of products designated as end-of-life / end-of-support by the vendor or publisher.

Motor Vehicles' use of non-vendor supported IT software increases the risk that existing vulnerabilities will persist in the related systems without the potential for patching or 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 IT software designated as end-of-life / end-of-support, which increases the difficulty of restoring system functionality if a technical failure occurs.

Motor Vehicles' Information Technology and Information Security Departments are aware of these IT software weaknesses and are currently working with the respective system vendors to develop solutions to upgrade the related End of Life software. System complexities and project prioritization have delayed appropriate solutions from being developed and implemented.

Our review noted three types of outdated IT software that we have communicated in detail to management in a separate document marked FOIAE under Section 2.2-3705.2 of the Code of Virginia, due to their sensitivity and description of security controls. Motor Vehicles should continue to dedicate the necessary resources to further develop plans to migrate off the unsupported IT software. Motor Vehicles should also transition off all unsupported software by either completely decommissioning unneeded software or upgrading to currently supported software as soon as possible.

Improve System Authentication Controls
Significant Deficiency

Motor Vehicles does not have appropriate authentication security controls implemented to reasonably protect one of its mission critical and sensitive systems.

The Security Standard requires that Motor Vehicles implement reasonably strong authentication mechanisms for all sensitive systems to protect authenticator content from unauthorized disclosure and modification.

Motor Vehicles implemented the current authentication system more than a decade ago, and has since not evaluated the related risk, or updated the legacy control mechanism to align with the requirements of the Security Standard.

Our review noted the related control weakness that we have communicated in detail to management in a separate document marked FOIAE under Section 2.2-3705.2 of the Code of Virginia, due to its sensitivity and description of security controls. Motor Vehicles should formally evaluate the risks associated with the currently implemented authentication security controls for the related system. Motor Vehicles should also update the related authentication controls to a more appropriately secure mechanism to better protect sensitive data and align with the Security Standard.

Improve Information Security Officer Independence
Significant Deficiency

Motor Vehicles does not position the Information Security Officer (ISO) role in an organizationally independent unit from the Chief Information Officer (CIO).

The Security Standard recommends that the ISO report directly to the agency head, where practical, and should not report to the CIO.

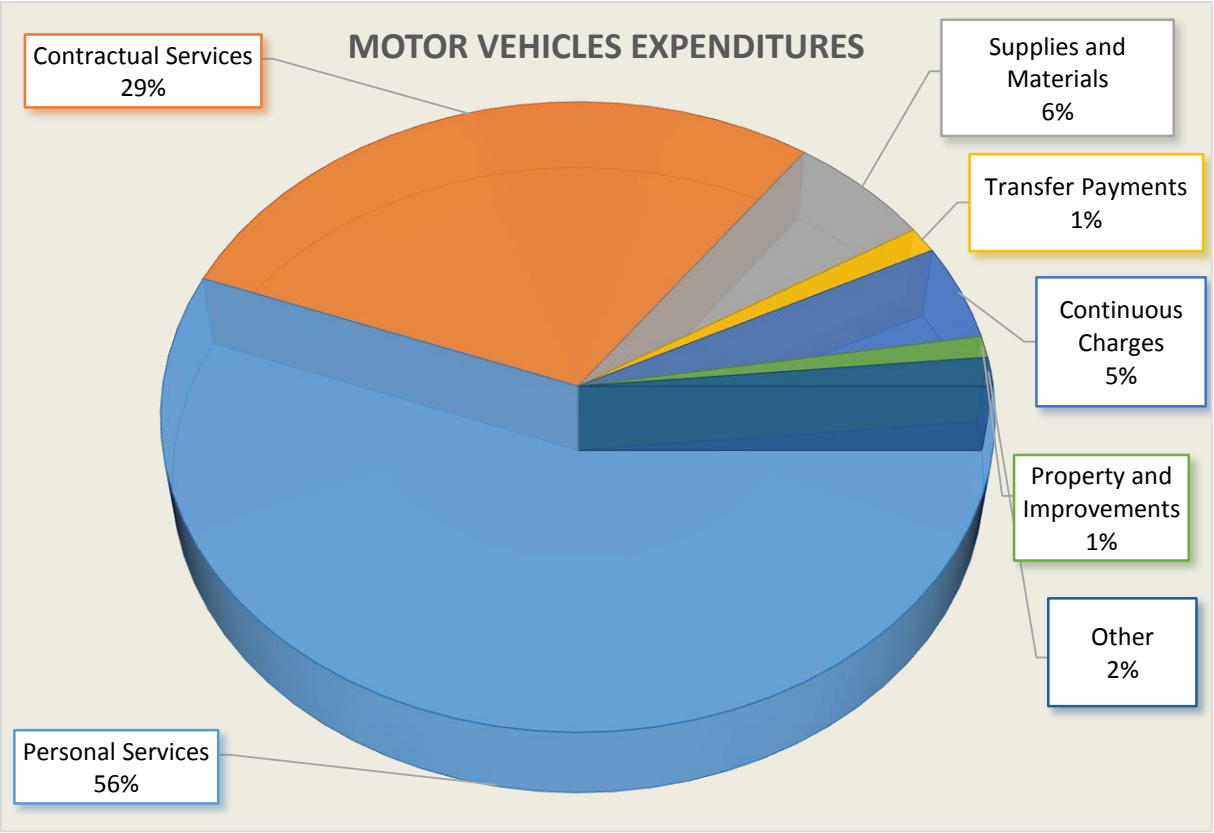
Having the ISO role reporting to the CIO may limit effective assessment and necessary recommendations of security controls, and assignment of security control responsibilities across the Motor Vehicles IT environment due to possible competing priorities that sometimes face the CIO.

In establishing its information security officer role within the organization, Motor Vehicles did not fully consider the need for full independence of the ISO and the CIO. The information security control weaknesses identified during this year's audit highlight the potential competing priorities of having the ISO report directly to the CIO.

Motor Vehicles should evaluate the organizational placement of the ISO to eliminate any conflicts of interest in the implementation of their information security program and controls. Motor Vehicles should also evaluate the timing of the separation of the ISO and CIO so as to not negatively impact significant IT and security projects that are currently ongoing. While it may not be feasible to have the ISO report directly to the agency head, Motor Vehicles should consider placing the ISO role in a different organizational unit reporting to another executive-level position.

Why the APA Audits Payroll and Human Resources

Motor Vehicles spends over $126 million, or 56 percent of its budget, on payroll and other personal service expenses including retirement contributions. Due to the significance of this activity, we consider payroll and human resource controls to be critical. These controls ensure both the accuracy of payroll and compliance with pension contribution requirements. We audited Motor Vehicle's practices against the requirements set by the Department of Accounts and the Virginia Retirement System. Subsequently, our testwork resulted in the following management recommendation.



Improve myVRS Navigator Reconciliation Process
Partial Repeat, Significant Deficiency

Motor Vehicles did not retain documentation that they properly reconciled the data in the Virginia Retirement System's (VRS) *my*VRS Navigator System to the agency's records monthly prior to certifying that the retirement data was correct. In addition, Motor Vehicles is not reviewing and resolving the errors from the Personnel Management Information System (PMIS) Cancelled Records Report prior to confirming that retirement contributions are correct.

The Commonwealth Accounting Policies and Procedures Manual Topic 50410 states that PMIS employers must review the PMIS Cancelled Record Report daily to ensure all information was recorded in *my*VRS Navigator. The same topic states that agencies should ensure that a timely review of the monthly reconciliation reports is performed and that employee enrollment information and any supporting documentation should be maintained for audit purposes.

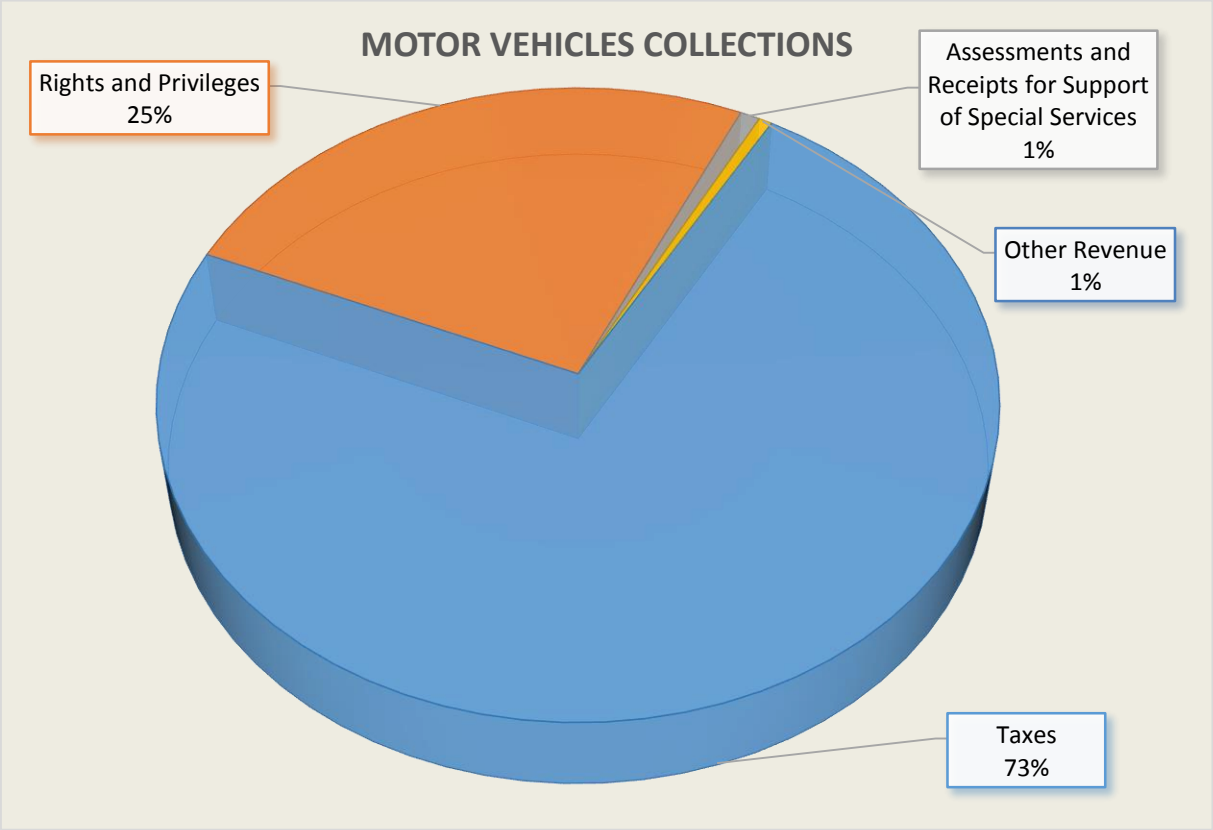
Without sufficient reconciliation documentation, there is no evidence that the monthly reconciliation of creditable compensation was actually performed, and therefore no way to know that the employees' retirement information in *my*VRS Navigator is accurate and in agreement with Motor Vehicles' records. By not reviewing the PMIS Cancelled Records Report, Motor Vehicles is unaware when information does not transmit correctly between the human resource system (PMIS) and the retirement system (*my*VRS Navigator) and; therefore, Motor Vehicles cannot not make appropriate corrections timely.

Management stated that verification of the agency's creditable compensation had been performed monthly, but the reports used from the agency's internal human resource system were not retained and could not be regenerated for inspection. In addition, Motor Vehicles was not certain if it or the Payroll Service Bureau was responsible for reviewing the PMIS Cancelled Record report.

Motor Vehicles' Human Resource Department should retain evidence that the data in *my*VRS Navigator was properly reconciled to the agency's employee records. PMIS Cancelled Record Reports should also be reviewed and any errors should be corrected timely.

Why the APA Audits Financial Reporting

Motor Vehicles collected over $2 billion in varied taxes and fees including, but not limited to, motor vehicle sales and use tax, fuels tax, fishing licenses, and birth certificates. As such, Motor Vehicles is individually material to the Commonwealth's Comprehensive Annual Financial Report (CAFR). We have audited the receipt of these funds and Motor Vehicle's financial reporting. Subsequently, our testwork resulted in the following two recommendations to management.



Create Processes for Review and Assessment of Third Party Vendors' Controls
Significant Deficiency

Motor Vehicles does not have policies and procedures in place to review and assess the effectiveness of third party vendors' (Provider) controls. As a result, Motor Vehicles is not ensuring that controls are reviewed and assessed for all significant Providers. Motor Vehicles uses Providers to collect major revenue sources, such as fuels taxes and vehicle sales and use taxes, and to collect and transfer sensitive information, such as personal information needed for vehicle registration. If

the controls at these Providers are not adequate, there is the risk that sensitive information is not properly protected or significant revenue amounts could be incorrect.

The Department of Accounts requires agencies to complete Agency Risk Management and Internal Control Standards (ARMICS) requirements and certifications, which include documenting, evaluating, and testing internal controls. This also applies to agency processes performed by Providers. Not properly monitoring the effective operation of internal controls at Providers reduces Motor Vehicles' ability to ensure that Providers' controls are adequate. In addition, the Security Standard considers Providers to be organizations that perform outsourced business tasks or functions on behalf of the Commonwealth. Section 1.1 of the Security Standard recognizes that agencies may procure information technology equipment, systems, and services covered by the Security Standard from Providers. In these situations, the Security Standard requires that agencies enforce the requirements outlined in the Security Standard through documented agreements with its Providers and oversight of the services performed.

Service Organization Control reports are evaluations performed at the Provider by an independent auditor using attestation standards established by the American Institute of Certified Public Accountants. The reports provide assurance over the design and effectiveness of the Provider's controls. Motor Vehicles has requested the reports for some Providers but the reports are not reviewed to ensure the Provider's controls are adequate, or to ensure that the report's complimentary controls, which detail controls needed to be in place at Motor Vehicles to have a complete control structure, are adequately implemented. In addition, most work areas at Motor Vehicles were not aware of the need to review Provider controls. The decentralized nature of Motor Vehicles creates a great need for an agency-wide understanding of Provider controls and the assessment of them.

Motor Vehicles' management should create a documented framework for identifying Providers and assessing Provider controls. This framework should include ensuring that contracts with the Providers require documented independent assurances over controls be provided as well as documenting the review of these assurances to determine effectiveness of Provider controls. This information should be provided to all areas of the agency.

Improve Procedures around Accounts Receivables Reporting
Significant Deficiency

Motor Vehicles has not created an accurate method of establishing an allowance for doubtful accounts for agency receivables. As a result, Motor Vehicles overstated the amount of their accounts receivable reported to the Department of Accounts for inclusion in the CAFR. The amount reported for accounts receivable included no allowance amount for approximately $1.4 million of fuels tax receivables that have been outstanding for more than a year, and are likely uncollectible.

Motor Vehicles did not include an allowance for fuels tax receivables because fuels taxes are a legal obligation and considered receivable even after a long period outstanding; therefore, management determined that no allowance needed to be created. In addition, the methodology for

the allowance for doubtful accounts reported for all other receivables was created more than five years ago by an employee who is no longer with the agency. Employees did not verify that this methodology was still reasonable. Management has not updated the allowance to reflect recent significant changes such as those made by the Transportation funding package passed in 2013.

Commonwealth Accounting Policies and Procedures Manual Topic 20505 states that management should establish an allowance for doubtful accounts, and the estimated allowance should be based on historical data or other pertinent information relative to the receivables in question. The topic goes on to state that uncollectible accounts may be written off of an agency's financial accounting records and no longer recognized as collectible receivables for financial reporting purposes, but the legal obligation to pay the debts still remains. Accounts written off remain debts of the agency until discharged by the Office of the Attorney General or collected.

Motor Vehicles has numerous streams of income relating to many different business functions. Individually, fuels tax receivables have continued to increase to material levels over the last several years. By not having an updated methodology for creating an estimate for the entire agency's uncollectible receivables, Motor Vehicles risks submitting overstated receivables information for inclusion in the CAFR.

Motor Vehicles' financial staff should create policies and procedures documenting the basis for the methodology of the allowance for doubtful accounts estimate, and regularly review the methodology especially when new transactions, regulatory changes, or any new conditions or events occur.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 15, 2015

The Honorable Terence R. McAuliffe
Governor of Virginia

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

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

Audit Objectives

Our audit's primary objective was to evaluate the accuracy of Agencies of the Secretary of Transportation's financial transactions as reported in the Comprehensive Annual Financial Report for the Commonwealth of Virginia for the year ended June 30, 2015, and test compliance for the Statewide Single Audit. In support of this objective, we evaluated the accuracy of recorded financial transactions in the Commonwealth Accounting and Reporting System and in each agency's accounting records, reviewed the adequacy of their internal control, tested for compliance with applicable laws, regulations, contracts, and grant agreements, and reviewed corrective actions of audit findings from prior year reports.

Audit Scope and Methodology

Management of the Agencies of the Secretary of Transportation have responsibility for establishing and maintaining internal control and complying with applicable laws and regulations. Internal control is a process designed to provide reasonable, but not absolute, assurance regarding the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws, regulations, contracts, and grant agreements.

We gained an understanding of the overall internal controls, both automated and manual, sufficient to plan the audit. We considered significance and risk in determining the nature and extent of our audit procedures. Our review encompassed controls over the following significant cycles, classes of transactions, and account balances.

Department of Motor Vehicles
- Accounts receivable and revenues
- Payroll and other expenses
- Financial reporting
- Information security and general system controls

Department of Transportation
- Accounts receivable and revenues
- Accounts payable and disbursements
- Capital asset management
- Cash and debt management
- Contract management
- Inventory
- Federal revenues, expenses and compliance for Highway Planning and Construction
- Information security and general system controls
- Payroll

The Department of Rail and Public Transportation, the Department of Aviation, Motor Vehicle Dealer Board, and Virginia Port Authority also fall under the control of the Secretary of Transportation. However, the Department of Rail and Public Transportation, the Department of Aviation, and Motor Vehicle Dealer Board are not material to the Comprehensive Annual Financial Report for the Commonwealth of Virginia, nor have a federal program that is required to be audited as part of the Statewide Single Audit. Additionally, the Virginia Port Authority was audited by other auditors and their report can be found at www.apa.virginia.gov. Accordingly, these agencies were not included in the scope of this audit.

We performed audit tests to determine whether the Agency's controls were adequate, had been placed in operation, and were being followed. Our audit also included tests of compliance with provisions of applicable laws, regulations, contracts, and grant agreements. Our audit procedures included inquiries of appropriate personnel, re-performance of automated processes, inspection of documents, records, contracts, reconciliations, board minutes, and observation of the Agencies' operations. We tested transactions and performed analytical procedures, including budgetary and trend analyses. We confirmed cash and investment balances with outside parties. Where applicable, we compared an agency's policies to best practices and Commonwealth standards.

Conclusions

We found that the Agencies of the Secretary of Transportation properly stated, in all material respects, the amounts recorded and reported in the Commonwealth Accounting and Reporting System and in other information reported to the Department of Accounts for inclusion in the Comprehensive Annual Financial Report for the Commonwealth of Virginia. The Agencies record their financial transactions on the cash basis of accounting, which is a comprehensive basis of accounting other than accounting principles generally accepted in the United States of America. The financial information presented in this report came directly from either the Commonwealth Accounting and Reporting System or other agency financial system.

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

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial information will not be prevented, or detected and corrected on a timely basis. We consider the deficiency entitled "Improve Controls over Financial Reporting" to be a material weakness for the Commonwealth.

A significant deficiency is a deficiency, or a combination of deficiencies in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We have explicitly identified 19 findings in the section titled "Audit Findings and Recommendations," as significant deficiencies for the Commonwealth.

As the findings noted above have been identified as a material weakness or significant deficiency for the Commonwealth, they will be reported as such in the Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of the Financial Statements Performed in Acccordance with Government Auditing Standards, included in the Commonwealth of Virginia Single Audit Report for the year ended 2015.

The Agencies have taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this letter.

Exit Conference and Report Distribution

We discussed this report with management on January 5 and 11, 2015. Management's response to the findings identified in our audit is included in the section titled "Agency Responses." We did not audit the agency responses and, accordingly, we express no opinion on it.

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

AUDITOR OF PUBLIC ACCOUNTS

JDE/alh

COMMONWEALTH of VIRGINIA

DEPARTMENT OF TRANSPORTATION
1401 EAST BROAD STREET
RICHMOND, VIRGINIA 23219-2000

Charles A. Kilpatrick, P.E.
Commissioner

January 14, 2016

Ms. Martha S. Mavredes
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23219

Dear Ms. Mavredes:

The Department of Transportation appreciates the opportunity to respond to the Commonwealth Transportation Fund audit for Fiscal Year 2015. Your review has identified opportunities for the Department to enhance its current practices to strengthen our internal controls, for which we give our highest level of attention and consideration. The Department has carefully reviewed the findings and developed corrective action plans to address the recommendations presented in the report and highlighted some of the areas of success in the areas mentioned in the audit. Our comments are summarized as follows:

Risk Alert
Upgrade or Decommission End-of-life Server Operating Systems

The Department shares APA's concerns regarding the need to continuously modernize and maintain our server environments. Over the past 15 months, Transportation's Information Technology Division has reduced the number of servers running end-of-life operating systems from 353 servers to 90 servers. Of the remaining 90 servers, immediate operating system upgrades are not possible as the impacted applications must be concurrently modernized to support the newer operating system. For applications and servers that are unable to be migrated or upgraded due to software limitations and/or other constraining dependencies, security exceptions will be filed with the Commonwealth Security office, until the application can be redeveloped and redeployed onto supported infrastructure or removed from operation.

To mitigate potential security vulnerabilities of these end-of-life applications, the Partnership along with Transportation has deployed the Enhanced Server Operating System Security "McAfee SolidCore" product to secure these servers against potential threats and other vulnerabilities. This software blocks potential attacks and is routinely monitored by the Partnership.

Improve Controls over Financial Reporting

The Department prepares over 60 financial submissions within a very short timeframe to support the Commonwealth's Comprehensive Annual Financial Report (CAFR). We appreciate APA's acknowledgement that the majority of our annual financial submissions were error free. The Department understands the importance of accurate reporting and the significance of VDOT's financial information to the CAFR and agrees that the quality of our reporting and internal review processes should be strengthened. The Department has developed detailed procedures for the preparation of the financial submissions, which were enhanced and updated in FY 2015, and each procedure contains a review process. The financial reporting procedures will be further strengthened for FY 2016 and will include an evaluation of timeframes and resources for both preparation and detailed quality control review of the submissions. Advance preparation procedures and automation will be employed wherever possible to provide more time for review and less chance for human error. We will also increase analytical procedures and reviews of variances to ensure they are reasonable and consistent across submissions. These enhancements should ensure accuracy of the annual financial information submitted to the Department of Accounts. It is important to recognize that these findings are related to financial reporting not the accuracy of the data. Our sound fiscal processes ensured the accurate recording of the agencies financial transactions.

Consider the Impact Funding has on Highway Infrastructure Capitalization

The Department concurs with APA on the importance of ensuring that legislation impacting our operations and funding is considered for financial reporting impacts, including the capitalization of infrastructure. The Department will formalize our existing process to identify legislative and other funding changes that could potentially impact the capitalization process through written documentation. The review process of new legislation will be documented annually and the capitalization process updated as required.

Develop and Implement IT Hardening Procedures

The Department agrees with the APA on the importance of hardening the servers supporting mission critical systems and ensuring that servers are deployed with the appropriate security configurations specific for the application. In collaboration with the Partnership, the Department follows ITRM Sec 501 standards for server hardening of systems designated as sensitive. Once the Partnership performs base hardening on servers, they are turned over for usage by Transportation. This process is referred to as

"on-boarding." Transportation performs additional hardening for sensitive systems and/or applications which are public-facing. However, those procedures are not always explicitly documented or logged. To mitigate this finding, we will formally document, approve, and log the completion of the Transportation IT hardening procedures and actions for infrastructure within our control by December 31, 2016.

Improve the Sensitive System Classification Process

The Department agrees with the auditor's recommendations and will enhance documentation of our sensitive system classification methodology by including the Information Security Officer's justification of the list of sensitive system ratings. We expect to have this enhancement implemented by December 31, 2016.

Improve Access Controls to IT Hardware

APA has reported that 207 personnel have access to the server room and this represents an excessive number. This number is inclusive of Transportation staff, to include security guards, facility engineers, electricians, and Systems Engineers, as well as Partnership staff. While the Department acknowledges that this number appears high, approved Partnership staff members were added at the direction of the Partnership to have the ability to address after hour emergencies and perform specialized IT services in response to urgent system outages. The need of having technical staff with varying expertise available and at "the ready" to support different platforms, is critical to the applications in which they are responsible for supporting.

Furthermore, the Department only allows badged personnel into the computer rooms who have undergone Virginia State Police background checks and who are approved and permitted by physical door security controls to enter the room. Any non-badged person needing access is approved by Transportation's Systems Engineering Manager and then escorted by a Transportation badged person, who is responsible for signing the door log stating the date and purpose of the visit. A review of personnel with computer room access, as well as door access logs will be performed. If anyone not requiring routine access to perform their job is identified, they will be removed by July 1, 2016.

Improve Vulnerability Scanning and Remediation Procedures

The Department agrees with the APA's finding to implement vulnerability scanning for our publicly facing and sensitive systems. To address this finding, Transportation will develop a plan to have our public-facing and/or sensitive systems scanned for vulnerabilities by August 31, 2016. We expect to have all public-facing and/or sensitive systems scanned by December 31, 2016, at which time a remediation plan will be developed to address significant vulnerabilities. Going forward, the Department will document and implement plans to have public-facing and/or sensitive systems scanned for vulnerabilities on a 90 day basis as directed by the ITRM Sec 501.

Upgrade End-of-Life Technology

As mentioned in our response to the Risk Alert, the Department shares APA's concerns regarding the need to continuously modernize and maintain our server environments. Of the remaining 90 servers operating on end-of-life technology, immediate operating system upgrades are not possible as the applications running on those servers must be concurrently modernized to support the newer operating system. For applications and servers that are unable to be migrated or upgraded due to software limitations and/or other constraining dependencies, security exceptions will be filed with the Partnership's Commonwealth Security office, until the application can be redeveloped and redeployed onto supported infrastructure or removed from operation. The Department is in the process of developing a remediation plan by August 31, 2016 that will identify the proposed corrective action on each of the 90 remaining end-of-life servers.

To mitigate potential security vulnerabilities of these end of life applications, the Partnership along with Transportation has deployed the Enhanced Server Operating System Security "McAfee SolidCore" product to secure these servers against potential threats and other vulnerabilities. This software blocks potential attacks and is routinely monitored by the Partnership.

Improve the Billing Process

The Department agrees that all billing should be performed timely, including bills handled outside of the normal automated process. We will strengthen our processes by documenting the procedures for manually processing invoices to federal agencies, monitoring the authorizations for federal projects and submitting requests for additional funds when estimated costs warrant the need for more funding. A backup person will be identified to support the function when the responsible person is absent, and appropriate monitoring processes will be implemented.

Improve the Process of Disclosing Economic Interests

The Department agrees that it is absolutely critical to have transparency and trust within state government operations. We have committed to taking the recommended corrective actions to reevaluate the positions within the agency designated to require a Statement of Economic Interest. The Department also emphasizes that the current agency positions were designated in accordance with Executive Order requirements of which require individual agency interpretation. As confirmed by APA staff, there are no established policies or procedures provided to Executive branch agencies beyond the Executive Order itself and as such, the development of VDOT policies and procedures as recommended by APA could establish a baseline for Executive branch agencies statewide. As shared by APA, this finding is being realized in multiple Executive branch agencies. It is the Department's desire that APA work with the Department of Human Resources Management, the Office of the Attorney General and the Ethics Commissioner to provide an overview of the related findings for all Executive branch agencies and to

work collaboratively together to provide additional guidance and direction for all Executive branch agencies.

Improve Access Controls to Payroll and HR Systems

The Department understands and agrees that access to information systems should be promptly removed upon termination. The Department will strengthen the internal controls over this process by performing more frequent reviews of employees with Payroll system access and identifying an additional Payroll Security Officer as a back-up. We will work with VDOT offices to ensure timely notification of employee transfers and terminations, to include working with the Department of Accounts to set up system termination dates in advance whenever possible.

Improve the Reconciliation to the Retirement System

The Department is committed to taking the recommended actions to revise existing practices for the reconciliation among three externally managed systems – the Commonwealth Integrated Personnel and Payroll System (CIPPS), the Personnel Management Information System (PMIS), and the Virginia Retirement System's (VRS) *my*VRS Navigator System. We must reemphasize our frustration in having to manually reconcile multiple systems that are not under VDOT control and do not logically speak to one another for data integration and service delivery. The Department was advised to reconcile and resolve exceptional errors on a monthly basis; yet, some of the required corrections were outside of our control, meaning that corrections to records were required by VRS. The Department has no control over VRS staff to force more timely corrections to records or in the delivery of needed data for the reconciliations. The Department has and continues to reach out and work in partnership with staff at the Department of Human Resources Management, the Virginia Retirement System and the Department of Accounts. It is our desire that APA will likewise share related findings across all agencies and that the noted external entities will work towards a personnel and financial system that is fully integrated.

I thank you and your staff for the assistance and guidance provided during this review. Your continued support and input is appreciated and will be used to improve the Department's internal controls.

Sincerely,

Charles A. Kilpatrick, P.E.
Commissioner

c: The Honorable Aubrey Layne
Chief Deputy Commissioner
Executive Staff

COMMONWEALTH of VIRGINIA
Department of Motor Vehicles
2300 West Broad Street

Richard D. Holcomb
Commissioner

Post Office Box 27412
Richmond, VA 23269-0001

January 19, 2016

Ms. Martha S. Mavredes
Auditor of Public Accounts
Post Office Box 125
Richmond, VA 23219

Dear Ms. Mavredes:

Thank you for this opportunity to respond to your latest audit of the Agencies of the Secretary of Transportation for the fiscal year ended June 30, 2015. We are pleased that you found our financial reporting to be properly stated. Furthermore, we sincerely appreciate the professionalism and guidance of your staff.

The corrective action plans we are proposing in response to your findings have been provided to your staff. Accordingly, DMV is working diligently to remediate the issues identified in the audit. We look forward to working with you in the future.

Please let me know if you have any questions or concerns.

Sincerely,

Richard D. Holcomb

RDH:dm

Phone: (804) 497-7100 TDD: 1-800-272-9268 Email: commish@dmv.virginia.gov Website: www.dmvNOW.com

AGENCY OFFICIALS

As of June, 2015

Aubrey L. Layne, Jr., Secretary of Transportation
Grindly Johnson, Deputy Secretary of Transportation
Nick Donohue, Deputy Secretary of Transportation

Department of Motor Vehicles
Richard D. Holcumb, Commissioner

Department of Transportation
Charles A. Kilpatrick, Commissioner

Department of Rail and Public Transportation
Jennifer Mitchell, Executive Director

Department of Aviation
Randall P. Burdette, Executive Director

Motor Vehicle Dealer Board
Bruce Gould, Executive Director

COMMONWEALTH TRANSPORTATION BOARD

Aubrey L. Layne, Jr., Chairman
Charles A. Kilpatrick, Vice-Chairman

Carlos M. Brown	John Malbon
Henry Connors, Jr.	John K. Matney
Alison DeTuncq	Jennifer Mitchell
James W. Dyke, Jr.	John F. Reinhart
William H. Fralin, Jr.	Court G. Rosen
Gary Garczynski	Shannon Valentine
E. Scott Kasprowicz	F. Dixon Whitworth, Jr.

Marty Williams

APPENDIX A
SUMMARY OF TRANSPORTATION AGENCY REVENUE SOURCES AND USES OF FUNDS

AGENCIES OF THE SECRETARY OF TRANSPORTATION
SUMMARY OF FINANCIAL INFORMATION
SOURCES AND USES
Cash Basis, For Fiscal Year 2015

	Department of Aviation	Department of Motor Vehicles	Department of Rail and Public Transportation	Department of Transportation	Motor Vehicle Dealer Board	Total Agencies of the Secretary of Transportation
Sources:	**2015**	**2015**	**2015**	**2015**	**2015**	**2015**
CTF Sources (net of refunds):						
Taxes	$ 29,546,511	$ 1,518,328	$ 313,629,670	$ 2,915,973,132	$ -	$ 3,260,667,641
Fees, licenses and permits	517,135	184,411,904	3,083,068	336,987,163	-	524,999,270
Tolls	-	-	-	34,295,457	-	34,295,457
Fines and assessments	4,496	21,857,089	27,540	9,517,143	-	31,406,269
Interest, dividends and rents	190,089	238,332	1,411,811	20,192,873	-	22,033,106
Federal grants and contracts	-	-	45,705,352	1,298,680,304	-	1,344,385,656
Other miscellaneous revenues	678,509	687,401	460,808	35,643,020	-	37,469,738
Receipts from cities, counties and towns	-	-	724,474	142,433,703	-	143,158,177
Revenue bond proceeds	-	-	-	300,298,025	-	300,298,025
Total CTF sources	30,936,741	208,713,053	365,042,722	5,094,020,823	-	5,698,713,339
Non-CTF Sources (net of refunds):						
General fund appropriations	(38,795)	-	-	(12,173,953)	-	(12,212,748)
Federal grants	354,184	-	-	-	-	354,184
Taxes	-	336,326	-	-	198,505	534,831
Fees, licenses, permits, fines and assessments	58,320	1,963,868	-	-	2,179,160	4,201,348
Other miscellaneous	-	159,695	-	4,251,389	1,938	4,413,021
Total non-CTF sources	373,709	2,459,889	-	(7,922,564)	2,379,602	(2,709,364)
Total sources	31,310,450	211,172,941	365,042,722	5,086,098,259	2,379,602	5,696,003,975
Net transfers in/(out)	251,426	(325,398)	156,964,512	(208,543,101)	395,688	(51,256,874)
Total funds available for use	$ 31,561,876	$ 210,847,544	$ 522,007,234	$ 4,877,555,157	$ 2,775,290	$ 5,644,747,101
Uses:						
Expenses (net of refunds):						
Administrative and support services	$ 2,175,937	$ 57,438,834	$ 7,201,780	$ 245,476,201	$ -	$ 312,292,752
Air transportation programs	4,728,063	-	-	-	-	4,728,063
Capital Outlay projects	-	2,818,143	-	10,699,727	-	13,517,870
Environmental monitoring and evaluation	-	-	-	11,603,513	-	11,603,513
Economic development activities	-	-	-	-	-	-
Financial assistance to localities	22,271,395	-	-	1,043,704,198	-	1,065,975,592
Ground transportation regulation	-	159,437,508	-	-	-	159,437,508
Ground transportation planning	-	-	3,893,903	60,960,265	-	64,854,168
Ground transportation safety	-	7,290,418	-	-	-	7,290,418
Highway acquisition and construction	-	-	-	1,729,845,376	-	1,729,845,376
Highway maintenance	-	-	-	1,479,836,794	-	1,479,836,794
Mass transit assistance	-	-	363,939,366	-	-	363,939,366
Debt service, principal and interest	-	-	-	316,932,138	-	316,932,138
Rail assistance	-	-	54,836,483	-	-	54,836,483
Regulation of professions and occupations	-	-	-	-	2,222,884	2,222,884
Toll facility operations	-	-	-	29,894,804	-	29,894,804
Total uses	$ 29,175,394	$ 226,984,904	$ 429,871,533	$ 4,928,953,016	$ 2,222,884	$ 5,617,207,730

Source: Commonwealth Accounting and Reporting System