



# AGENCIES OF THE SECRETARY OF TRANSPORTATION

## REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2023

Auditor of Public Accounts

Staci A. Henshaw, CPA

[www.apa.virginia.gov](http://www.apa.virginia.gov)

(804) 225-3350



## AUDIT SUMMARY

This report summarizes our fiscal year 2023 audit results for the Virginia Department of Transportation (Transportation) and the Department of Motor Vehicles (Motor Vehicles). Collectively, these two agencies spent \$7.7 billion or 82 percent of the total expenses and collected 98 percent of revenues for the agencies under the Secretary of Transportation.

Our audits of these agencies, which support our work on the Commonwealth's Annual Comprehensive Financial Report (ACFR) for the year ended June 30, 2023, found:

- proper recording and reporting of all transactions, in all material respects, in the Commonwealth's accounting and reporting system, each agency's internal accounting and reporting system, and supplemental information and attachments submitted to the Department of Accounts (Accounts);
- matters involving internal control and its operation necessary to bring to management's attention at Transportation and Motor Vehicles;
- instances of noncompliance with applicable laws and regulations or other matters at Transportation and Motor Vehicles that are required to be reported; and
- adequate corrective action with respect to prior audit findings and recommendations classified as complete in the [Findings Summary](#) included in the Appendix.

This report includes a Risk Alert applicable to Motor Vehicles that requires the action and cooperation of management at Motor Vehicles and the Virginia Information Technologies Agency (VITA). Our separate audit of VITA will provide more details on the issue noted in this alert.

In the section titled "Internal Control and Compliance Findings and Recommendations," we have included our assessment of the conditions and causes resulting in the internal control and compliance findings identified through our audits as well as recommendations for addressing those findings. Our assessment does not remove management's responsibility to perform a thorough assessment of the conditions and causes of the findings and develop and appropriately implement adequate corrective actions to resolve the findings as required by the Department of Accounts in Topic 10205 – Agency Response to APA Audit of the Commonwealth Accounting Policies and Procedures Manual. Those corrective actions may include additional items beyond our recommendations.

## - TABLE OF CONTENTS -

	<u>Pages</u>
AUDIT SUMMARY	
INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS	1-9
Department of Transportation	1-5
Department of Motor Vehicles	6-8
RISK ALERT	9
Department of Motor Vehicles	9
INDEPENDENT AUDITOR'S REPORT	10-13
APPENDIX – FINDINGS SUMMARY	14
AGENCY RESPONSES	15-19
Department of Transportation	15-17
Department of Motor Vehicles	18-19

## INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

This section groups findings by agency, and each finding includes information about the type and the severity classification of the finding. For findings reported in a prior year, the finding's header provides the first year it was issued along with the prior year title(s), where applicable. The section titled "Independent Auditor's Report" includes additional details on the severity classifications.

While we test financial reporting and related internal controls, both manual and automated, this year our recommendations for Transportation and Motor Vehicles relate only to information and physical security, including system access reviews. Both agencies collect, manage, and store significant volumes of financial and personal data within their mission-critical systems. Because of the critical nature of this data, management at both agencies must take the necessary precautions to ensure the availability, integrity, and security of the data within their systems. We compared the agencies' practices to those required by the Commonwealth's Information Security Standard, SEC 501 (Security Standard), Security Audit Standard, SEC 502 (IT Audit Standard), the Commonwealth's IT Risk Management Standard, SEC 520 (IT Risk Management Standard), and the Commonwealth's Hosted Environment Information Security Standard, SEC 525 (Hosted Environment Security Standard) and offer the following recommendations.

### DEPARTMENT OF TRANSPORTATION

#### **Improve Offboarding Process**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

**First Issued:** Fiscal Year 2020

**Titles of Related Prior Findings:** "Ensure Supervisors are Completing the Separating Employee Checklist" and "Ensure Timely Removal of Access to the Commonwealth's Accounting and Financial Reporting System"

Transportation's current offboarding process is not an effective control for meeting its operational and compliance objectives. As currently designed, supervisors initiate the offboarding process, but then several divisions throughout the department are responsible for successfully executing offboarding tasks. Supervisors at Transportation are to confirm they have initiated these tasks by completing the Employee Separation/Transfer Checklist; however, Human Resources could not provide a completed checklist for eight of 37 (22%) applicable terminated employees tested. Additionally, because of delays in starting the offboarding process and untimely notifications, staff of the Office of Information Security could not remove access to the Commonwealth's network timely for 19 of 35 (54%) terminated employees tested who had access. On average, these 19 employees retained access 12 days after termination. An additional six employees retained access to the Commonwealth's accounting and financial reporting system an average of 20 days after termination because Human Resources did not receive timely separation notifications. Furthermore, district badging offices did not terminate physical badge access for 16 of 36 (44%) applicable terminated employees because they did not receive timely separation notifications. On average, these employees retained their physical access 40 days after termination.

Management is responsible for an internal control system that is effective at meeting operational and compliance objectives. Management designs policies and procedures to fit an entity's circumstances and implements them as an integral part of the entity's operations. The Commonwealth's Security Standard, Section PS-4 Personnel Termination, requires that an organization disable an individual's information system access within 24 hours of employment termination. Without an effective offboarding process, Transportation increases the risk that former employees will use their unremoved access to cause harm.

Transportation manages approximately 8,000 employees in a decentralized environment across the entire Commonwealth with a current process that is not effective at offboarding individuals in a manner that meets operational and compliance objectives. However, in fiscal year 2023, Transportation implemented a new internal human resources management system and is currently working to re-engineer its business processes to streamline certain tasks related to offboarding using the new system. Management from Human Resources, the Office of Information Security, and the Office of Safety, Security and Emergency Management should collaborate to ensure business process re-engineering efforts related to offboarding are effective at meeting the operational and compliance needs of Transportation. Lastly, management within these divisions should establish and implement activities to monitor the new offboarding process, evaluate the results, and make operational adjustments as needed.

### **Improve Database Security**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

Transportation does not secure one of its databases in accordance with its internal policies, the Commonwealth's Security Standard, and industry best practices, such as the Center for Internet Security Benchmarks (best practices). We communicated three control weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms.

The Security Standard requires Transportation to implement certain security controls to safeguard systems that contain or process sensitive data. By not meeting the minimum requirements in the Security Standard and industry best practices, Transportation cannot ensure the confidentiality, integrity, and availability of data within its system.

Transportation did not secure one of its databases in accordance with the Security Standard and best practices because it did not follow its internal policies and procedures. Additionally, Transportation's internal policies did not clarify certain requirements for separation of duties and audit logging and monitoring, which led to the control weaknesses identified in the communication marked FOIAE. Transportation should take the actions recommended in the communication marked FOIAE to increase Transportation's security posture and help protect the confidentiality, integrity, and availability of sensitive and mission-critical data.

### **Upgrade End-of-Life Technology**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

Transportation uses end-of-life technology on one of its information technology (IT) systems that process mission-essential data without an approved exception. We communicated the control weakness to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms.

The Security Standard prohibits agencies from using software that is end-of-life, and which the vendor no longer supports, to reduce unnecessary risk to the confidentiality, integrity, and availability of the Transportation's information systems and data. If Transportation is not able to update its software to a supported version due to compatibility or other operational issues, the Security Standard requires the agency head to submit an exception request for approval to the Commonwealth's Chief Information Security Officer (Security Standard, Sections SI-2-COV Flaw Remediation, SA-22 Unsupported System Components, and 1.5 Exceptions to Security Requirements).

Transportation should submit an exception for running end-of-life technology that includes a description of compensating controls that will reduce the software vulnerability risk. The exception request should also include Transportation's plan to upgrade the systems running outdated and unsupported software. Properly managing risk related to end-of-life technology will increase Transportation's security posture and help protect the confidentiality, integrity, and availability of sensitive and mission-critical data.

### **Conduct IT Risk Assessments and Develop System Security Plans**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

Transportation does not conduct some aspects of its IT risk management documentation in accordance with the IT Risk Management Standard. IT risk management documentation includes identification of Transportation's data, analysis of the sensitivity of and risks to its data, as well as plans to protect IT systems. Specifically:

- Transportation has not conducted a risk assessment in the last three years for 21 of its 24 (88%) sensitive systems as required; however, Transportation was able to provide evidence that it completed risk assessments in the past four to six years for 17 of its 24 (71%) sensitive systems. The Security Standard and IT Risk Management Standard require Transportation to conduct and document a risk assessment for each sensitive system no less than once every three years and conduct an annual self-assessment to determine the continued validity of the risk assessment (Security Standard, Section 6.2 Risk Assessment; IT Risk Management Standard, Section 4.5.3 Performance of Risk Assessments). By not conducting risk assessments for sensitive systems in a timely manner, Transportation may not adequately identify risks for its sensitive systems or identify and implement appropriate

security controls for its IT systems and environment to address those risks. Unaddressed system security risks can lead to a potential compromise of Transportation’s sensitive information.

- Transportation does not consistently develop and review System Security Plans (SSPs). Specifically, Transportation has not developed an SSP for four of its 24 (17%) sensitive systems as required and has not reviewed and updated the SSPs annually for 17 of its 24 (71%) sensitive systems. Transportation did develop an SSP for three of its 24 sensitive systems in 2023; however, the SSP template Transportation used to develop these SSPs did not include certain elements of information, such as backup schedules and the system’s security requirements. The Security Standard and IT Risk Management Standard require that Transportation develop an SSP for each information system based on the results of the risk assessment, including all existing and planned IT security controls for the system (Security Standard, Section PL-2 System Security Plan; IT Risk Management Standard, Section 4.6 System Security Plan). Without developing and documenting SSPs for each sensitive system, Transportation cannot demonstrate if proper information security controls are in place. Additionally, developing SSPs without the required elements increases Transportation’s risk that it will not effectively identify a potential risk and implement the security controls needed to protect its sensitive system environment (Security Standard, Section PL-2 System Security Plan).

Transportation prioritized developing and implementing the new risk management documentation process, which contributed to Transportation not completing all risk assessments and SSPs timely. With the implementation of the new process, Transportation plans to combine the risk assessments with the SSPs for each of the 24 sensitive systems to create a single risk management document to maintain.

Transportation should conduct and document a risk assessment for each of its sensitive systems to identify risks and vulnerabilities and develop and document SSPs with the security controls needed to address the identified risks. Additionally, Transportation should maintain updated risk assessments and SSPs by conducting annual reviews and self-assessments as required by the Security Standard and IT Risk Management Standard. Implementing corrective action will help protect the confidentiality, integrity, and availability of sensitive and mission-critical data.

**Continue Improving Service Provider Oversight**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

**First Issued:** Fiscal Year 2021

Transportation continues not to consistently monitor its third-party Software as a Service (SaaS) providers that fall under VITA’s Enterprise Cloud Oversight Service (ECOS). Transportation uses VITA’s ECOS to assist with gaining assurance that its SaaS providers implement the minimum-security controls required by the Hosted Environment Security Standard. Specifically, Transportation has not received independent audit assurance reports for three of its 19 (16%) SaaS providers under active ECOS

oversight. Transportation also has not documented its review and evaluation of the independent audit assurance reports received for the remaining 16 SaaS providers under active ECOS oversight.

Transportation has made progress since the prior audit by developing a process to track monthly compliance reports and annual independent audit reports received from ECOS. However, the new process does not include documenting Transportation’s review and evaluation of each independent audit assurance report. Transportation follows the Hosted Environment Security Standard, which requires the organization to employ appropriate processes, methods, and techniques to monitor security control compliance for service providers on an ongoing basis (Hosted Environment Security Standard, Section SA-9(c)). Without reviewing and evaluating the independent audit assurance reports and consistently managing its third-party SaaS providers, Transportation cannot validate that its SaaS providers implement the required controls to protect Transportation’s sensitive and confidential data.

Transportation prioritized updating and implementing the new process that documents when Transportation receives and reviews monthly compliance reports and communicates with ECOS regarding any issues. Additionally, the new process documents when independent audit assurance reports are due. However, Transportation’s process does not include the requirement to document the review and evaluation of each annual independent audit assurance report.

Transportation should consistently obtain, review, and evaluate each independent audit assurance report from ECOS for each SaaS provider. Transportation should also update and implement a process that includes the expectation to document the review and evaluation of each independent audit assurance report received and follow-up with ECOS regarding control deficiencies identified in the reports. Proper review and evaluation of SaaS provider assurance reports will help maintain the confidentiality, integrity, and availability of sensitive and mission-critical data.

### **Improve Change Control Process**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

**First Issued:** Fiscal Year 2022

Transportation has made progress towards implementing certain elements in its change and configuration management process as required by the Security Standard. However, we communicated one remaining weakness remains to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

The Security Standard requires change and configuration management controls to appropriately protect sensitive systems. Without implementing certain change and configuration management controls, Transportation may be unable to properly manage changes to its systems to ensure data integrity and system recovery. Transportation should update its change and configuration management process to address the weakness discussed in the communication marked FOIAE to protect the confidentiality, integrity, and availability of sensitive and mission-critical data.



## DEPARTMENT OF MOTOR VEHICLES

### **Implement a Process to Annually Review User Access**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

While Motor Vehicles has documented a process for annually reviewing user access to one of its sensitive information systems, it has not implemented that process nor provided data owners with access listings to evaluate and certify that users still require access to the system. The Security Standard, Section 8.1. AC2 Account Management, requires that organizations review access for compliance with account management requirements on an annual basis. Not performing annual reviews of access accounts for Motor Vehicles' sensitive information system in compliance with the Security Standard creates an elevated risk of individuals retaining unreasonable access to sensitive information that they can use for unofficial activity.

Motor Vehicles has not completed implementing the process of performing access reviews in accordance with the documented procedures due to challenges caused by other information systems that interface with the sensitive information system. These interfacing systems make it difficult for Motor Vehicles to develop reports with the information that data owners will need to ensure compliance with the principle of least privilege. Motor Vehicles should implement its process for annually reviewing user access to its sensitive information system in accordance with the Security Standard.

### **Improve Database Security**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

**First Issued:** Fiscal Year 2022

Motor Vehicles does not meet some minimum-security controls and configurations to protect a database that supports sensitive and mission-critical web applications in accordance with Motor Vehicles' Security and Risk Management Standard and the Security Standard. We communicated the weaknesses and recommendations to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. The Security Standard requires organizations to implement certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of Motor Vehicles' information systems and data.

Motor Vehicles did not prioritize implementing certain security mechanisms. By not meeting the requirements of the Motor Vehicles' Security and Risk Management Standard and the Security Standard, Motor Vehicles increases risk related to data confidentiality, integrity, and availability. Motor Vehicles should continue its efforts to remediate the identified weaknesses to help maintain the confidentiality, integrity, and availability of Motor Vehicles' sensitive and mission-critical data.

### **Improve Web Application Security Controls**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

Motor Vehicles does not secure a sensitive web application with some of the minimum-security controls required by the Security Standard. We communicated the weakness to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms.

The Security Standard requires organizations to implement certain controls that reduce unnecessary risk to the confidentiality, integrity, and availability of Motor Vehicles' information systems and data. By not meeting the requirements of the Security Standard, Motor Vehicles increases its risk related to data confidentiality, integrity, and availability.

Due to an oversight, an employee did not perform certain control activities we communicated to management. Motor Vehicles should dedicate the necessary supervision to ensure employees are fulfilling their responsibilities to aid Motor Vehicles in meeting the minimum requirements in the Security Standard. Addressing these weaknesses will help to ensure the confidentiality, integrity, and availability of sensitive and mission-critical data and compliance with the Security Standard.

### **Continue to Update End-of-Life Technology**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

**First Issued:** Fiscal Year 2021

Motor Vehicles made progress in upgrading the end-of-life (EOL) technologies identified during fiscal year 2022; however, Motor Vehicles continues to run EOL technologies on its IT systems. Motor Vehicles maintains technologies that support mission essential and critical applications that run software that its vendors no longer support. We communicated the control weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms.

The Security Standard prohibits agencies from using software that is EOL, and which the vendor no longer supports, to reduce unnecessary risk to the confidentiality, integrity, and availability of Motor Vehicle's information systems and data. Motor Vehicles did not update, replace, or decommission the EOL software due to procurement delays.

Motor Vehicles should dedicate the necessary resources to evaluate and implement the controls and recommendations discussed in the communication marked FOIAE in accordance with the Security Standard. Decommissioning EOL software will help to ensure that Motor Vehicles secures its IT environment and systems to protect its sensitive and mission-critical data.

### **Conduct Timely IT Security Audits**

**Type:** Internal Control and Compliance

**Severity:** Significant Deficiency

Motor Vehicles does not conduct a comprehensive IT security audit on each sensitive system at least once every three years that assesses whether IT security controls are adequate and effective. We communicated the weakness to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms.

The Security Standard, Section 7, requires that each IT system classified as sensitive undergo an IT security audit as required by and in accordance with the current version of the IT Audit Standard. The IT Audit Standard, Section 1.4, requires that IT systems containing sensitive data, or systems with an assessed sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall receive an IT security audit at least once every three years. Additionally, the IT Audit Standard, Section 2.2, requires that the IT Security Auditor shall use criteria that, at a minimum, assess the effectiveness of the system controls and measure compliance with the applicable requirements of the Security Standard.

Without conducting comprehensive IT security audits that cover all applicable Security Standard requirements for each sensitive system every three years, Motor Vehicles increases the risk that IT staff will not detect and mitigate existing weaknesses. Malicious parties taking advantage of continued weaknesses could compromise sensitive and confidential data. Further, such security incidents could lead to mission-critical systems being unavailable.

Motor Vehicles was not able to conduct timely IT security audits because it experienced employee turnover and a lack of response for required information. Additionally, one of its systems is undergoing a major upgrade and another is encountering technical issues, which are contributing to delays in conducting IT security audits. Management should evaluate potential options and develop a formal process for conducting IT audits over each sensitive system at least once every three years that test the effectiveness of the IT security controls and compliance with Security Standard requirements. Motor Vehicles should then complete the planned IT security audits, either through its internal audit function or through the acquisition of external third-party services. Compliance with the IT Audit Standard will help to ensure the confidentiality, integrity, and availability of sensitive and mission-critical data.

## RISK ALERT

During our audit, we encountered internal control and compliance issues that are beyond the corrective action of Motor Vehicles' management alone and require the action and cooperation of management at VITA. The following issue represents such a risk to Motor Vehicles and the Commonwealth during fiscal year 2023.

### DEPARTMENT OF MOTOR VEHICLES

#### **Unpatched Software**

**First Issued:** Fiscal Year 2021

VITA contracts with various providers to create the Commonwealth's Information Technology Infrastructure Services Program (ITISP) to provide agencies with installation, maintenance, operation, and support of IT infrastructure components, such as servers, routers, firewalls, and virtual private networks. Motor Vehicles continues to rely on contractors procured by VITA for the installation of security patches in systems that support Motor Vehicles' operations. Additionally, Motor Vehicles relies on VITA, as the contract administrator, to maintain oversight and enforce the contract agreements with the ITISP contractors. As of July 2023, the ITISP contractors had not applied certain security patches that are critical and highly important to Motor Vehicles' IT infrastructure components, which are past the 90-day update window allowed by the Security Standard.

The Security Standard requires the installation of security-relevant software updates within 90 days of release. The Security Standard does allow for varying time periods depending on factors such as the criticality of the update, but generally the ITISP uses a 90-day window from the date of release as its standard for determining timely implementation of security patches (Security Standard, Section SI-2 Flaw Remediation). Missing system security updates increase the risk of successful cyberattack, exploitation, and data breach by malicious parties.

While VITA is responsible for enforcing the service level agreement, it has not been able to compel the current ITISP contractors to install certain security patches to Motor Vehicles' IT infrastructure components to remediate vulnerabilities in a timely manner or taken actions to obtain these required services from another source. Motor Vehicles' is working with VITA and the ITISP contractors to ensure that the ITISP contractors install critical and highly important security patches as required. Additionally, our separate audit of VITA's contract management will continue to report on this issue.



Staci A. Henshaw, CPA  
Auditor of Public Accounts

# Commonwealth of Virginia

*Auditor of Public Accounts*

P.O. Box 1295  
Richmond, Virginia 23218

December 15, 2023

The Honorable Glenn Youngkin  
Governor of Virginia

Stephen C. Brich, Commissioner  
Department of Transportation

Joint Legislative Audit  
and Review Commission

Gerald Lackey, Commissioner  
Department of Motor Vehicles

W. Sheppard "Shep" Miller, III  
Secretary of Transportation

We have audited the financial records and operations of the **Agencies of the Secretary of Transportation** for the year ended June 30, 2023. We conducted this audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, in support of the Commonwealth's Annual Comprehensive Financial Report audit. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## **Audit Objectives**

Our audit's primary objective was to evaluate the accuracy of the Agencies of the Secretary of Transportation's financial transactions as reported in the Annual Comprehensive Financial Report for the Commonwealth of Virginia for the year ended June 30, 2023. In support of this objective, we evaluated the accuracy of recorded financial transactions in the Commonwealth's accounting and financial reporting system, each agency's internal accounting and reporting system, and supplemental information and attachments submitted to the Department of Accounts (Accounts); reviewed the adequacy of each agency's internal control; tested for compliance with applicable laws, regulations, contracts, and grant agreements; and reviewed corrective actions with respect to audit findings and recommendations from prior year reports.

## **Audit Scope and Methodology**

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

We gained an understanding of the overall internal controls, both automated and manual, sufficient to plan the audit. We considered materiality 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 Transportation (Transportation)*

- Accounts payable and expenses
- Accounts receivable and revenues
- Capital asset balances
- Cash and debt balances
- Commonwealth's retirement benefits system
- Contract procurement and management
- Financial reporting
- Human resources
- Information security and general system controls (including access controls)
- Inventory
- Payroll and other expenses

### *Department of Motor Vehicles, including Department of Motor Vehicles Transfer Payments (Motor Vehicles)*

- Accounts payable and transfer payment expenses
- Accounts receivable and revenues
- Commonwealth's retirement benefits system
- Financial reporting
- Information security and general system controls (including access controls)

The following agencies under the control of the Secretary of Transportation are not material to the Annual Comprehensive Financial Report for the Commonwealth of Virginia or are audited by other auditors. As a result, these agencies are not included in the scope of this audit:

- Department of Aviation
- Department of Rail and Public Transportation
- Motor Vehicle Dealer Board
- Office of Intermodal Planning and Investment

Office of Public-Private Partnerships  
Virginia Commercial Space Flight Authority  
Virginia Passenger Rail Authority  
Virginia Port Authority

We performed audit tests to determine whether each 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, inspection of documents, records, and contracts, and observation of the agencies' operations. We performed analytical procedures, including budgetary and trend analyses, and tested details of transactions to achieve our audit objectives. We also confirmed cash with outside parties.

A nonstatistical sampling approach was used. Our samples were designed to support conclusions about our audit objectives. An appropriate sampling methodology was used to ensure the samples selected were representative of the population and provided sufficient, appropriate evidence. We identified specific attributes for testing each of the samples and, when appropriate, we projected our results to the population.

Our consideration of internal control over financial reporting (internal control) was for the limited purpose described in the section "Audit Objectives" and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control as described in the section titled "Internal Control and Compliance Findings and Recommendations," that we consider to be significant deficiencies.

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 or noncompliance 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 statements will not be prevented or detected and corrected on a timely basis. 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.

## **Conclusions**

We found that Transportation and Motor Vehicles properly stated, in all material respects, the amounts recorded and reported in the Commonwealth's accounting and financial reporting system, each agency's internal accounting and reporting system, and supplemental information and attachments submitted to Accounts.

We noted certain matters involving internal control and its operation and compliance with applicable laws, regulations, contracts, and grant agreements that require management’s attention and corrective action. These matters are described in the section titled “Internal Control and Compliance Findings and Recommendations.”

Transportation and Motor Vehicles have taken adequate corrective action with respect to audit findings identified as complete in the [Findings Summary](#) included in the Appendix.

Since the findings noted above include those that have been identified as significant deficiencies, they will be reported as such in the “Independent Auditor’s Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of the Financial Statements Performed in Accordance with Government Auditing Standards,” which is included in the Commonwealth of Virginia’s Single Audit Report for the year ended June 30, 2023. The Single Audit Report will be available at [www.apa.virginia.gov](http://www.apa.virginia.gov) in February 2024.

### **Exit Conference and Report Distribution**

We provided management of Transportation and Motor Vehicles with a draft of this report on February 5, 2024, for review and development of their responses. Government Auditing Standards require the auditor to perform limited procedures on the agencies’ responses to the findings identified in our audit, which are included in the accompanying section titled “Agency Responses.” The agencies’ responses were not subjected to the other auditing procedures applied in the audit and, accordingly, we express no opinion on the responses. Additionally, VITA was made aware of the risk alert and will respond to the issue in its separately issued audit report anticipated to be released in February 2024.

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.

Staci A. Henshaw  
AUDITOR OF PUBLIC ACCOUNTS

GDS/vks



## FINDINGS SUMMARY

Finding Title	Agency	Status of Corrective Action	Year First Issued
Improve Access Controls to the Commonwealth's Purchasing System	Transportation	Complete	2022
Improve Internal Controls Surrounding Granting and Removing Access for Equipment Systems	Transportation	Complete	2022
Continue Developing a Process to Annually Review User Access to a Sensitive Information System	Motor Vehicles	Complete	2022
Improve Offboarding Process <sup>1</sup>	Transportation	Ongoing	2020
Improve Database Security	Transportation	Ongoing	2023
Upgrade End-of-Life Technology	Transportation	Ongoing	2023
Conduct IT Risk Assessments and Develop System Security Plans	Transportation	Ongoing	2023
Continue Improving Service Provider Oversight	Transportation	Ongoing	2021
Improve Change Control Process	Transportation	Ongoing	2022
Implement a Process to Annually Review User Access	Motor Vehicles	Ongoing	2023
Improve Database Security	Motor Vehicles	Ongoing	2022
Improve Web Application Security Controls	Motor Vehicles	Ongoing	2023
Continue to Update End-of-Life Technology	Motor Vehicles	Ongoing	2021
Conduct Timely IT Security Audits	Motor Vehicles	Ongoing	2023

<sup>1</sup> Titles of Related Prior Findings: "Ensure Supervisors are Completing the Separating Employee Checklist" and "Ensure Timely Removal of Access to the Commonwealth's Accounting and Financial Reporting System."



## COMMONWEALTH of VIRGINIA

### DEPARTMENT OF TRANSPORTATION

Stephen C. Brich, P.E.  
Commissioner

1401 East Broad Street  
Richmond, Virginia 23219

(804) 786-2701  
Fax: (804) 786-2940

February 6, 2024

Ms. Staci Henshaw  
Auditor of Public Accounts  
Post Office Box 1295  
Richmond, Virginia 23219

Dear Ms. Henshaw:

The Department of Transportation appreciates the opportunity to respond to the Secretary of Transportation's audit report for Fiscal Year 2023. Below is the Department's response which should address the areas of concern:

#### **Improve Offboarding Process**

Transportation has implemented a new human capital management system, which automates the process for separation checklists. Human Resources is focused on improving system functionality and re-engineering our offboarding process to streamline certain tasks through system notifications. The Human Resource Division will work with the other divisions and executives to communicate the importance and requirement of supervisors to complete the separation checklists and ensure all access is removed from employees within 24 hours of separation. The Human Resource Division will update existing training materials, develop new job aids when needed and provide training to supervisors on the separation checklist process in the system.

#### **Improve Database Security**

Transportation understands the importance of securing sensitive infrastructure and will mitigate risk by implementing an established enterprise audit logging process for this database which will ensure that logs to be reviewed by business staff are not accessible by database administrators. Changes to this system will be required to flow through Transportation's updated change control process which will ensure that the necessary system configuration baseline documentation is attached before any changes to the system are moved to production.

VirginiaDOT.org  
WE KEEP VIRGINIA MOVING

### **Upgrade End-Of Life Technology**

Transportation had prepared a security exception and submitted it to VITA timely; however, the delay was due to not receiving VITA CISO approval. VITA raised questions and provided feedback that required VDOT to produce more detailed project plans and provide additional compensating controls for the EOL technology. Transportation has now addressed these items and the exception has been re-submitted to VITA. Assuming no additional issues are identified, we anticipate VITA approving the security exception no later than the end of March 2024.

### **Conduct IT Risk Assessments and Develop System Security Plans**

Transportation continues to work towards currency in the risk assessment program using updated risk assessment tools and processes. Transportation plans to be current with the Risk Assessment Plan by June 30, 2024. Transportation plans to complete the new risk assessment and system security plan process for all sensitive systems by December 31, 2024. Additionally, Transportation will be issuing a new Risk Assessment policy document that details risk assessment and system security plan requirements which will vary based on system sensitivity. This is planned for completion by September 30, 2024.

### **Continue Improving Service Provider Oversight**

Transportation instituted the monthly VDOT ECOS compliance report as the agreed upon action from the prior year APA audit. To address the additional concerns raised, Transportation has added a section to the monthly VDOT ECOS compliance report that indicates the audit firm opinion for the SOC2 audit. Unmodified “clean” opinions will be considered by Transportation as acceptable to support continued use as a third party hosted supplier, while modified or adverse opinions will be considered unacceptable and require an IT project to move to a different supplier; this has been completed. Transportation will also document an internal ECOS policy to further codify the above requirements; this will be completed by September 2024.

### **Improve Change Control Process**

Transportation understands the importance of change control processes and will further tighten the change control documentation process by implementing management control points. Within Transportation’s current change control process, we will add action steps for ensuring that the necessary system configuration baseline documentation is attached before any system changes are moved to production.

Ms. Henshaw  
February 6, 2024  
Page 3

We appreciate the professionalism and guidance provided by your staff and look forward to working with you next year.

Sincerely,

A handwritten signature in blue ink, appearing to read "Stephen C. Brich".

Stephen C. Brich, P.E.  
Commissioner

c: The Honorable Sheppard Miller III  
Executive Staff



**Gerald F. Lackey, Ph.D.**  
Commissioner

**COMMONWEALTH of VIRGINIA**  
Department of Motor Vehicles

2300 W. Broad St.  
P.O. Box 27412  
Richmond, VA 23269-0001  
(804) 497-7100  
TTY: 711 or (800) 828-1120  
dmv.virginia.gov

January 30, 2024

Ms. Staci A. Henshaw  
Auditor of Public Accounts  
Post Office Box 1295  
Richmond, VA 23218

Dear Ms. Henshaw:

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, 2023. We are pleased that you found our financial reporting to be properly stated. We also sincerely appreciate the professionalism and guidance of your staff. The Department of Motor Vehicles' responses to the findings are below.

Implement a Process to Annually Review User Access

The Department of Motor Vehicles has started the annual review using the new process and will include this in our start of year tasks.

Continue to Update End-of-Life Technology

The Department of Motor Vehicles understands the need to update or replace end of life software and the risk that it creates to the agency by not doing so. The team will prioritize resources to be more proactive and addressing end of life and end of support software.

Improve Database Security

The Department of Motor Vehicles understands the need to perform timely patching of our databases and we'll assign the necessary resources to meet compliance for this and recovery testing.

Conduct Timely IT Security Audits

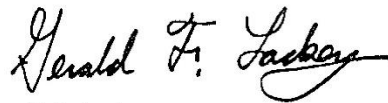
The Department of Motor Vehicles understands the need to perform audits on sensitive IT systems and is taking steps to ensure compliance with the IT audit plan and the requirements of VITA security standards.

Improve Web Application Security Controls

The Department of Motor Vehicles has already started a new process to verify the backups of our critical IT infrastructure and is starting the work to perform restoration tests on a scheduled basis.

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,

A handwritten signature in black ink that reads "Gerald F. Lackey". The signature is written in a cursive style with a large, sweeping "G" and "L".

Gerald F. Lackey