


DEPARTMENT OF MOTOR VEHICLES

REPORT ON AUDIT
FOR THE YEAR ENDED
JUNE 30, 2025

Auditor of Public Accounts
Staci A. Henshaw, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

Our audit of the Department of Motor Vehicles (Motor Vehicles) for the year ended June 30, 2025, found:

- proper recording and reporting of all transactions, in all material respects, in the Commonwealth's accounting and reporting system, Motor Vehicles' internal accounting and reporting system, and supplemental information and attachments submitted to the Department of Accounts (Accounts);

- matters involving internal control and its operation requiring management's attention that also represent instances of noncompliance with applicable laws and regulations that are required to be reported under Government Auditing Standards; however, we do not consider them to be material weaknesses; and

- adequate corrective action with respect to prior audit findings identified as complete in the Findings Summary included in the Appendix.

Additionally, our report includes one risk alert that requires the action and cooperation of Motor Vehicles' management and the Virginia Information Technologies Agency (VITA) regarding risks related to unpatched software.

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 audit 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 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-

INTERNAL CONTROL FINDINGS AND RECOMMENDATIONS

Improve Vulnerability Management
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Issued: Fiscal Year 2024

Motor Vehicles continues not to remediate vulnerabilities affecting its information technology (IT) environment in accordance with its Security and Risk Management Standard (Risk Management Policy), as well as the Commonwealth's Information Security Standard, SEC530 (Security Standard), and the Commonwealth's IT Risk Management Standard, SEC520 (Risk Management Standard). While Motor Vehicles updated its Risk Management Policy since the prior year's audit to align with the requirements outlined in the Security Standard and Risk Management Standard, Motor Vehicles did not remediate certain vulnerabilities older than 30 days as of June 2025 classified with a severity of critical or high.

Motor Vehicles' Risk Management Policy requires Motor Vehicles to remediate vulnerabilities within 30 days in accordance with an organizational assessment of risk. The Security Standard requires Motor Vehicles to remediate legitimate vulnerabilities within 30 days unless otherwise specified by Commonwealth Security Risk Management (CSRM) in accordance with an organizational assessment of risk. The Risk Management Standard requires Motor Vehicles to "fix vulnerabilities within 30 days of a fix becoming available that are either rated as critical or high or otherwise identified by CSRM." Additionally, the Risk Management Standard requires Motor Vehicles to remediate all other vulnerabilities within 90 days of a fix becoming available and acquire an approved security exception for the vulnerability should Motor Vehicles not remediate it within the timeframes identified.

Software vulnerabilities are publicly known flaws that bad actors may exploit and use to circumvent organizational information security controls to infiltrate a network or application. The longer these vulnerabilities exist in an environment, the higher the risk of compromise and unauthorized access to sensitive and mission-critical systems and data. It is therefore imperative for organizations to respond quickly and mitigate these publicly known flaws as soon as possible. Without timely vulnerability remediation and appropriate software patching, Motor Vehicles increases the risk of unauthorized access to sensitive and mission-critical systems.

Motor Vehicles is unable to remediate the known vulnerabilities within the required timeframe as it has not yet implemented its new vulnerability management process due to other competing priorities. Motor Vehicles should dedicate resources as necessary to mitigate legitimate vulnerabilities affecting its IT environment within the timeframe required by its Risk Management Policy, the Security Standard, and the Risk Management Standard. If Motor Vehicles is unable to mitigate vulnerabilities within the required timeframe, it should apply for an extension from CSRM that is supported by an organizational assessment of risk. Timely remediation of significant vulnerabilities will help protect the confidentiality, integrity, and availability of Motor Vehicles' sensitive and mission-critical information.

Improve Change and Configuration Management
Type: Internal Control and Compliance
Severity: Significant Deficiency

Motor Vehicles does not implement certain IT change and configuration management requirements in accordance with its IT change and configuration management policies and procedures and the Security Standard. We communicated four 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 defines certain requirements that Motor Vehicles must implement for its IT change and configuration management process. By not meeting the requirements of the Security Standard, Motor Vehicles increases risk related to data confidentiality, integrity, and availability. A lack of oversight to enforce its policies and procedures and delays with an ongoing project led to the weaknesses identified in the communication marked FOIAE.

Motor Vehicles should improve oversight of its IT change and configuration management process to ensure staff comply with its internal policies, procedures, and the Security Standard. Additionally, Motor Vehicles should continue dedicating the necessary resources to complete the ongoing project to implement certain controls. Implementing these changes will help to resolve the weaknesses identified in the communication marked FOIAE and maintain the confidentiality, integrity, and availability of Motor Vehicles' sensitive and mission-critical data.

Improve Physical and Environmental Security
Type: Internal Control and Compliance
Severity: Significant Deficiency

Motor Vehicles does not define certain requirements in its Joint Operations Center Physical Security Policy (Security Policy) nor implement certain physical and environmental security controls in accordance with its Security Policy and the Security Standard. We communicated three 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 requires Motor Vehicles to implement certain controls to safeguard its IT systems and infrastructure assets that contain sensitive and mission-critical data. By not meeting the requirements of the Security Standard, Motor Vehicles increases risk related to data confidentiality, integrity, and availability. Staffing constraints, competing priorities, and a lack of sufficient oversight led to the weaknesses communicated in the communication marked FOIAE.

Motor Vehicles should prioritize resources to implement the minimum physical and environmental security controls identified in the communication marked FOIAE and revise its policies to meet the Security Standard's requirements. Implementing the required physical and environment

security controls will help Motor Vehicles maintain the confidentiality, integrity, and availability of Motor Vehicles' sensitive and mission-critical data.

Improve Web Application Security
Type: Internal Control and Compliance
Severity: Significant Deficiency

Motor Vehicles does not implement certain minimum security controls and configurations to protect the web application that supports its financial accounting system in accordance with its policy and the Security Standard. Motor Vehicles also does not align certain policy requirements in accordance with the requirements of the Security Standard. We communicated six weaknesses 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 Motor Vehicles to implement certain security mechanisms to protect applications and systems. By not meeting the requirements of the Security Standard, Motor Vehicles increases risk related to data confidentiality, integrity, and availability.

Management did not ensure that Motor Vehicles implemented application configuration consistent with its baseline configurations policy. Additionally, they did not ensure that Motor Vehicles' policies comply with the Security Standard requirements. Collectively, these actions led to the weaknesses identified in the communication marked FOIAE. Management should prioritize resources to implement the minimum security controls and configurations and revise Motor Vehicles' policies to align with the Security Standard's requirements to help maintain the confidentiality, integrity, and availability of Motor Vehicles' sensitive and mission-critical data.

Improve Policies and Procedures to Ensure Compliance with the Conflict of Interest Act
Type: Internal Control and Compliance
Severity: Significant Deficiency

Motor Vehicles is not properly identifying individuals in a position of trust and tracking their completion of required disclosures or training to ensure compliance with the State and Local Government Conflict of Interest Act (COIA) requirements. Motor Vehicles identified two individuals within the Commonwealth's human resources system as needing to submit a Statement of Economic Interest (SOEI) form; however, Motor Vehicles did not ensure these employees submitted the required form. Additionally, two employees in current positions of trust were not identified by Motor Vehicles and as such they did not file the required disclosure. Further, Motor Vehicles has no procedures for tracking which employees have completed required COIA training.

Per § 2.2-3114 of the Code of Virginia, persons occupying positions of trust within state government or non-salaried citizen members of policy and supervisory boards shall file a disclosure statement with the Commonwealth's Conflict of Interest Ethics Advisory Council (Council), as a condition

to assuming office or employment, and thereafter shall file such a statement annually on or before February 1. Code of Virginia § 2.2-3130 requires that each employee within a position of trust complete COIA training within two months of their hire date and at least once every two years after the initial training. Further, per § 2.2-3129 of the Code of Virginia, the state agency is responsible for maintaining records of training attendance for its employees.

Without appropriately identifying employees in positions of trust and ensuring completion of required training, Motor Vehicles could be susceptible to actual or perceived conflicts of interest and may limit its ability to hold its employees accountable for not knowing how to recognize and resolve a conflict of interest. Employees could be subject to penalties for inadequate disclosure on their filings, as outlined within §§ 2.2-3120 through 2.2-3127 of the Code of Virginia.

The Motor Vehicles COIA Coordinator stated that they followed Executive Order 18 to determine which employees should complete the SOEI at Motor Vehicles; this order specifically identifies agency positions that should file the SOEI form annually. However, this order is "[i]n furtherance of the purposes of" the Conflict of Interests Act; as such, the filing requirements should not be limited to these individuals and should include all individuals identified as being in a position of trust. Additionally, the COIA Coordinator believed that the Council was responsible for tracking training completions and monitoring for compliance; however, this is the responsibility of each state agency. While Motor Vehicles has documented policies and procedures over the COIA, the policies and procedures do not sufficiently address the Coordinator's responsibilities for ensuring that the requirements are properly met.

Motor Vehicles should revise its written policies and procedures covering COIA to ensure that all individuals in a position of trust are properly identified and notified of the submission and training requirements. Further, Motor Vehicles should improve its procedures for internally tracking, monitoring, and communicating these requirements to its employees.

RISK ALERT

During the course of our audit, we encountered issues that are beyond the corrective action of Motor Vehicles' management alone and require the action and cooperation of management and the Virginia Information Technology Agency (VITA). The following issues represent such a risk to Motor Vehicles and the Commonwealth.

Unpatched Software

First Reported: Fiscal Year 2021

VITA contracts with various providers, collectively known as 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 2025, the ITISP contractors had not applied a significant number of security patches that are critical and highly important to Motor Vehicles' IT infrastructure components, all of which are past the 30-day update window allowed by the Security Standard.

The Security Standard requires the installation of security-relevant software and firmware updates within 30 days of release or within a timeframe approved by VITA's Commonwealth Security and Risk Management division. 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 30-day window from the date of release as its standard for determining timely implementation of security patches. Missing system security updates increases the risk of successful cyberattack, exploit, 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 to remediate vulnerabilities in a timely manner or take 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 all critical and highly important security patches on all servers. Additionally, our separate audit of VITA's contract management will also continue to report on this issue.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 12, 2025

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

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

Gerald Lackey, Commissioner
Department of Motor Vehicles

We have audited the financial records and operations of the **Department of Motor Vehicles** (Motor Vehicles) for the year ended June 30, 2025. 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 Motor Vehicles' financial transactions as reported in the Annual Comprehensive Financial Report for the Commonwealth of Virginia for the year ended June 30, 2025. In support of this objective, we evaluated the accuracy of recorded financial transactions in the Commonwealth's accounting and financial reporting system, Motor Vehicles' internal accounting and reporting system, and supplemental information and attachments submitted to the Department of Accounts (Accounts); reviewed the adequacy of Motor Vehicles' 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 reports.

Audit Scope and Methodology

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

We gained an understanding of the overall internal controls, both automated and manual, sufficient to plan the audit. We considered 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:

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

We performed audit tests to determine whether Motor Vehicles' 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 and records, and observation of Motor Vehicles' operations. We performed analytical procedures, including budgetary and trend analyses, and tested details of transactions to achieve our audit objectives.

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 titled "Improve Vulnerability Management," "Improve Change and Configuration Management," "Improve Physical and Environmental Security," "Improve Web Application Security," and "Improve Policies and Procedures to Ensure Compliance with the Conflict of Interest Act," which are 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 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 Motor Vehicles properly stated, in all material respects, the amounts recorded and reported in the Commonwealth's accounting and financial reporting system, Motor Vehicles' 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."

Motor Vehicles has taken adequate corrective action with respect to prior 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, 2025. The Single Audit Report will be available at www.apa.virginia.gov in February 2026.

Exit Conference and Report Distribution

We provided management of Motor Vehicles with a draft of this report for review on January 16, 2026. Government Auditing Standards require the auditor to perform limited procedures on Motor Vehicles' response to the findings identified in our audit, which is included in the accompanying section titled "Agency Response." Motor Vehicles' response was not subjected to the other auditing procedures applied in the audit and, accordingly, we express no opinion on the response.

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	Status of Corrective Action*	Fiscal Year First Reported
Improve Database Security	Complete	2022
Conduct Timely IT Security Audits	Complete	2023
Implement a Process to Annually Review User Access	Complete	2023
Improve Vulnerability Management	Ongoing	2024
Improve Change and Configuration Management	Ongoing	2025
Improve Physical and Environmental Security	Ongoing	2025
Improve Web Application Security	Ongoing	2025
Improve Policies and Procedures to Ensure Compliance with the Conflict of Interest Act	Ongoing	2025

*A status of **Complete** indicates management has taken adequate corrective action. A status of **Ongoing** indicates new and/or existing findings that require management's corrective action as of fiscal year end.

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

February 11, 2026

Ms. Staci A. Henshaw
Auditor of Public Accounts
P. O. Box 1295
Richmond, Virginia 23218

Dear Ms. Henshaw:

Thank you for the opportunity to respond to the latest audit of the agencies of the Secretary of Transportation. We appreciate the professionalism and guidance of your staff. The responses from the Department of Motor Vehicles to the findings are below.

Improve Physical and Environmental Security

DMV has reviewed and updated its Joint Operations Center Physical Security Policy to align with SEC530 and implemented monthly reviews of facility access lists and visitor access logs as required. A risk assessment is underway in coordination with the ongoing datacenter migration; however, completion will extend beyond June 2026 due to dependencies on the migration timeline.

Improve Change and Configuration Management

DMV has implemented process improvements including using our dedicated testing team workflow to ensure proper segregation of duties and change closure tracking through weekly Change Advisory Board (CAB) reviews. A standardized security impact analysis template has been incorporated into the change management process, and audit logging/monitoring capabilities will be implemented as part of the migration. Full remediation is targeted for completion by June 2026 in advance of the FY26 follow-up review.

Improve Vulnerability Management

DMV acknowledges this finding and has engaged SAIC/VITA in a remediation project to address the underlying causes, including inaccurate asset inventory and non-functional agents on certain devices. We are conducting weekly meetings with our vendor to ensure all in-scope assets have proper patch management. Inventory cleanup is targeted for

completion by February 15, 2026, with full compliance to the 30-day vulnerability remediation standard expected within 60 days thereafter.

Improve Web Application Security

DMV has updated its Risk Management Standard to align with SEC530 and completed configuration updates. Configuration baseline monitoring is currently being implemented, and automated backup testing will be established within 90 days. All remediation activities will be completed prior to the FY26 follow-up review.

Unpatched Software

DMV has escalated this finding to appropriate VITA leadership, as timely patching of DMV's infrastructure is under VITA's operational control. The timeline for remediation is uncertain due to the ongoing transition from the incumbent to a new vendor, which may involve toolset changes. DMV will continue to monitor VITA's progress and coordinate with VITA leadership to ensure vulnerabilities are remediated within required timeframes.

Improve Policies and Procedures to Ensure Compliance with the Conflict of Interest Act

DMV has clarified the responsibilities of the agency's Conflict of Interest Act (COIA) Coordinator and implemented internal controls to ensure employees in positions of trust are properly identified and notified of training and statement of economic interest submission requirements. Using Executive Order 18, the COIA Coordinator identified all responsible employees. In December, the coordinator created a spreadsheet to track the SOEI training for filers at DMV. The training spreadsheet will allow the coordinator to reach out to the filers to ensure training is completed on time in the future.

DMV will be working with the Department of Accounts on our corrective actions regarding these findings. Please let me know if you have any questions or concerns.

Sincerely,

Gerald F. Lackey

Gerald F. Lackey, PhD