



DEPARTMENT OF MOTOR VEHICLES

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2024

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, 2024, 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 necessary to bring to management's attention that also represent instances of noncompliance with applicable laws and regulations or other matters 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.

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.

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 fiscal year 2023, we included the results of our audit of Motor Vehicles in the report titled "[Agencies of the Secretary of Transportation for the Year Ended June 30, 2023](#)."

- TABLE OF CONTENTS -

Pages

AUDIT SUMMARY

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

1-4

RISK ALERT

4-5

INDEPENDENT AUDITOR'S REPORT

6-8

APPENDIX – FINDINGS SUMMARY

9

AGENCY RESPONSE

10-11

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Vulnerability Management

Type: Internal Control and Compliance

Severity: Significant Deficiency

The Department of Motor Vehicles (Motor Vehicles) does not remediate vulnerabilities affecting its information technology (IT) environment in accordance with the Commonwealth's Information Security Standard, SEC530 (Security Standard), and the Commonwealth's IT Risk Management Standard, SEC520 (Risk Management Standard). Specifically, as of September 2024, Motor Vehicles did not remediate a significant number of vulnerabilities in its IT environment classified with a severity of critical or high and numerous vulnerabilities classified with a severity of medium or low, which Motor Vehicles detected in its vulnerability scans in June 2024. Additionally, management did not update Motor Vehicles' Security and Risk Management Standard (Security and Risk Management Policy) to align with the current requirements of the Security Standard and Risk Management Standard, as it continues to reflect outdated requirements for scanning for and mitigating vulnerabilities within 90 days.

The Security Standard requires Motor Vehicles to "monitor and scan for vulnerabilities in the system and hosted applications at least once every 30 days, and when new vulnerabilities potentially affecting the system are identified and reported." The Security Standard also 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 according to the National Vulnerability Database 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 vulnerabilities as soon as possible. Without timely vulnerability scans and appropriate software patching, Motor Vehicles increases the risk of unauthorized access to sensitive and mission-critical systems.

Motor Vehicles has experienced issues with the vulnerability scanning tool since January 2023, causing the agency to not be aware of the vulnerabilities affecting its IT environment for over a year. While the vulnerability scanning tool was fixed by June 2024, Motor Vehicles was not scanning all IT assets due to ongoing issues with the tool not detecting all IT assets. Motor Vehicles was able to detect some vulnerabilities starting in June 2024 but has been unable to remediate the known vulnerabilities due to limited staffing resources that had to focus on other higher priorities. Additionally, while Motor Vehicles updated its Security and Risk Management Policy in February 2024, Motor Vehicles did not

update the required timeframes for conducting vulnerability scans and mitigating vulnerabilities due to an oversight during the revision process.

Motor Vehicles should review and revise its Security and Risk Management Policy to ensure its vulnerability management process aligns with the requirements outlined in the Security Standard and Risk Management Standard. Motor Vehicles should also implement its process to mitigate legitimate vulnerabilities affecting its IT environment within the timeframe required by the Security Standard and the Risk Management Standard. If Motor Vehicles is unable to mitigate vulnerabilities within the required timeframe, it should request an extension approval 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.

Implement a Process to Annually Review User Access

Type: Internal Control and Compliance

Severity: Significant Deficiency

First Reported: Fiscal Year 2023

While Motor Vehicles has documented a process for annually reviewing user access to one of its sensitive information systems, it has not fully implemented that process nor provided data owners with access listings to evaluate and certify that each user still requires access to the system or initiate the process to have a user's access disabled or modified. The Security Standard requires that organizations review access for compliance with account management requirements on an annual basis. Not performing annual access reviews of accounts for Motor Vehicles' sensitive information system in compliance with the Security Standard creates an elevated risk of individuals retaining unnecessary access to sensitive information that they can use for unofficial activity.

Motor Vehicles has not completed its implementation of performing access reviews in accordance with its documented procedures due to challenges encountered. During its Spring 2024 review, Motor Vehicles discovered that it needed to consider other access controls within the system before proceeding. Due to the dependency of access controls, Motor Vehicles is still refining and implementing its review process with an expected resolution by Fall 2024.

Motor Vehicles should continue to refine and implement its process for annually reviewing user access to its sensitive information system in accordance with the Security Standard. Implementing an adequate process for reviewing user access annually will help ensure the confidentiality and integrity of Motor Vehicles' sensitive information.

Improve Database Security

Type: Internal Control and Compliance

Severity: Significant Deficiency

First Reported: Fiscal Year 2022

Motor Vehicles continues to not implement minimum security controls and configurations to protect a database that supports sensitive and mission-critical web applications in accordance with the Security Standard. Since the fiscal year 2023 audit, Motor Vehicles remediated one of the two weaknesses, and we communicated the remaining weakness 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 Motor Vehicles to implement certain security mechanisms to protect databases. By not meeting the requirements of the Security Standard, Motor Vehicles increases risk related to data confidentiality, integrity, and availability.

Motor Vehicles' lack of planning and prioritizing the security mechanisms led to the weaknesses identified in the communication marked FOIAE. Motor Vehicles should plan and prioritize implementing the security mechanisms to meet the Security Standard's requirements and help maintain the confidentiality, integrity, and availability of Motor Vehicles' sensitive and mission-critical data.

Conduct Timely IT Security Audits

Type: Internal Control and Compliance

Severity: Significant Deficiency

First Reported: Fiscal Year 2023

Motor Vehicles continues to not conduct a comprehensive IT security audit on each sensitive system at least once every three years. An IT security audit assesses whether IT security controls are adequate and effective. Specifically, Motor Vehicles has nine internal sensitive systems subject to the IT security audit requirements of the Commonwealth's IT Security Audit Standard, SEC502 (IT Audit Standard); three of which Motor Vehicles did not audit in the last three years. Additionally, two of the audits that Motor Vehicles conducted in the last three years, did not include an assessment of some controls that the IT Audit Standard requires to be audited. As a result, Motor Vehicles did not conduct a comprehensive IT security audit for five of its nine (56%) internal sensitive systems in the last three years.

The IT Audit Standard requires Motor Vehicles to assess IT systems that contain sensitive data or reside in a system with a sensitivity of high for confidentiality, integrity, or availability at least once every three years or more frequently commensurate with risk. Additionally, the IT Audit Standard requires that the IT Security auditor use criteria that assess the effectiveness of the system controls and measure compliance with the applicable requirements of the Commonwealth's IT Resource Management Policies and Standards.

By not conducting comprehensive IT security audits that cover all applicable security control requirements for each sensitive system every three years, Motor Vehicles increases the risk that it will not detect and mitigate existing weaknesses. Malicious parties may take advantage of weaknesses to compromise sensitive and confidential data. Further, such security incidents could lead to mission-critical systems becoming unavailable.

Motor Vehicles did not make progress in conducting IT security audits for its remaining systems due to turnover in its Internal Audit Department and not identifying that some audits did not cover the required IT security controls. Motor Vehicles entered an agreement in August 2024 with VITA's IT Security Audit Service to conduct security audits for the duration of three years beginning in fiscal year 2025. Motor Vehicles should continue working with VITA to conduct IT security audits for each sensitive system at least once every three years to test the effectiveness of the IT security controls and compliance with the Security Standard.

RISK ALERT

During the course of our audit, we encountered an issue that is beyond the corrective action of Motor Vehicles' management alone and requires the action and cooperation of management and VITA. The following issue represents such a risk to Motor Vehicles and the Commonwealth.

Unpatched Software

First Reported: 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 2024, the ITISP contractors had not applied a significant number of security patches that are critical 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 CSRM 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 increase 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. Our separate audit of VITA's contract management will also 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 9, 2024

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, 2024. 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, 2024. 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 the 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 year 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, records, and contracts, 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 and federal compliance (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," "Implement a Process to Annually Review User Access," "Improve Database Security," and "Conduct Timely IT Security Audits," 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 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 or material noncompliance with a type of compliance requirement of a federal program 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 and recommendations 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, 2024. The Single Audit Report will be available at www.apa.virginia.gov in February 2025.

Exit Conference and Report Distribution

We provided management of Motor Vehicles with a draft of this report for review on January 27, 2025. Government Auditing Standards require the auditor to perform limited procedures on the agency's 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/clj

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	First Reported for Fiscal Year
Continue to Update End-of-Life Technology	Complete	2021
Improve Web Application Security Controls	Complete	2023
Improve Vulnerability Management	Ongoing	2024
Implement a Process to Annually Review User Access	Ongoing	2023
Improve Database Security	Ongoing	2022
Conduct Timely IT Security Audits	Ongoing	2023

* A status of **Complete** indicates management has taken adequate corrective action. **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 6, 2025

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

Dear Ms. Henshaw:

Thank you for this opportunity to respond to your latest audit of the Department of Motor Vehicles for the fiscal year ended June 30, 2024. 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.

Conduct Timely IT Security Audits

To ensure the timely completion of IT security audits, we have engaged a third-party firm to address all outstanding audits. Currently, only two out of the eleven audits remain, and they are scheduled for completion by June 2025.

Moving forward, we have outsourced our IT audit requirements to VITA and will coordinate with them to schedule future audits efficiently.

Improve Database Security

To address the audit findings and strengthen our database security, the agency has taken decisive steps to enhance both policy and operational practices. These actions ensure compliance with industry standards and reinforce our commitment to maintaining a secure IT environment. The key measures implemented include:

- 1. Policy Updates:** The agency has updated its internal security policies to align with the new SEC 530 security standard, as authored by VITA. This update has been completed.
- 2. Vulnerability Patching:** The agency is committed to patching all database vulnerabilities within 30 days of the manufacturer's release. To ensure compliance, the CISO is collaborating with the CIO on a burndown schedule, providing ongoing oversight and monitoring of patching.

Improve Vulnerability Management Process

To strengthen our vulnerability management process and address the audit findings, the agency has taken targeted actions to improve oversight, coordination, and compliance. These measures are designed to enhance our ability to promptly identify and remediate critical vulnerabilities, ensuring a more secure IT environment. The key steps include:

- **Dedicated Oversight:** A staff member within Information Security & Risk Management has been assigned to oversee vulnerability management activities.
- **Enhanced Coordination:** This individual will guide and support internal IT staff, as well as collaborate with VITA and their vendors to ensure proper configuration of management platforms.
- **Timely Patching Compliance:** Increased oversight and coordination efforts are aimed at ensuring that all critical vulnerabilities are patched within the required timeframe.

These actions reinforce our commitment to maintaining a robust and compliant vulnerability management process.

Implement a Process to Annually Review User Access

To strengthen access controls and ensure compliance with security best practices, the agency has conducted a comprehensive review of user access. During this process, we identified that several front-end systems control access to mainframe records, necessitating a simultaneous audit of these systems to ensure thorough coverage.

Now that the review is complete, we are actively working to reduce the number of legacy or unnecessary accounts. This cleanup effort is currently in progress, with an expected completion by late spring of 2025.

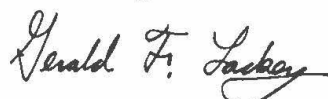
These actions reinforce our commitment to maintaining a secure and well-managed access control environment.

Unpatched Software

The agency is actively addressing the risk of unpatched software through continuous collaboration with VITA and their vendors. This ongoing partnership ensures that their platforms are effectively scanning for vulnerabilities and applying necessary patches to maintain system security.

By working closely with VITA, we are committed to maintaining a proactive approach to software patching, reducing security risks, and ensuring compliance with industry standards.

Sincerely,



Gerald F. Lackey, PhD