Audit Highlights

Highlights of performance audit report on the Department of Motor Vehicles, Information Security issued on September 10, 2024.

Legislative Auditor report # LA24-08.

Background

The mission of the Department of Motor Vehicles (DMV) is to become a vehicle services national leader by providing efficient motor vehicle solutions for the identification, licensure, and protection of those they serve. The DMV was founded in 1957 and at the time of this audit had more than 1,100 employees of which 65 were information technology employees.

Currently the DMV licenses over 2.3 million Nevada drivers and identification card holders and registers more than 2.7 million vehicles while maintaining the integrity and privacy of DMV records.

The DMV processes approximately 10 million transactions and collects $1.6 billion in revenue each year. The DMV is comprised of seven operational divisions, each orchestrated under the authority of the Director's Office.

The DMV is currently in the early stages of a digital transformation effort. Over the next few years, the DMV will move many of its services online in an effort to rebuild its customer service delivery and information technology platforms.

Purpose of Audit

The purpose of the audit was to determine if the DMV has adequate information security controls in place to protect its information processing systems. The audit included the systems and practices in place during fiscal years 2022 and 2023. We also reviewed information back to 2020 for user access and 2021 for asset inventory.

Audit Recommendations

This audit report contains 17 recommendations to improve information security controls over data security, inventory, risk assessments, critical policies, and user access for systems and applications.

The DMV accepted the 17 recommendations.

Recommendation Status

The DMV's 60-day plan for corrective action is due on December 9, 2024. In addition, the 6-month report on the status of audit recommendations is due on June 9, 2025.

Department of Motor Vehicles

Information Security

Summary

The DMV has not adequately prioritized critical information technology (IT) functions to mitigate service disruptions, ensure timely recovery, and safeguard data. For instance, policies and plans governing IT operations, including an IT operation risk assessment, continuity of operations, disaster recovery, incident response plans, and general IT-related policies were either not completed or not followed when necessary. Furthermore, DMV's data is vulnerable since the data destruction and patch management processes do not track or monitor hard drives needing data sanitization or necessary software updates. The DMV does not monitor the data extraction process used for data sales or review audit logs when changes are made to sensitive information in its primary application. Adequate IT policies protect entities from unnecessary security exposure and prolonged system failure recovery.

In addition, the DMV has not fully implemented controls over user access to ensure systems and applications are protected from unauthorized access. For instance, Information Technology Security (ITSEC) forms are not always updated with relevant information. Some users in the same position have more access than others without any record of why that is, including local administrator access. In addition, the DMV is not regularly reviewing current user access or permissions as required by state security standards. Furthermore, the DMV is not reconciling its IT assets, including hardware and software, leaving many discrepancies across inventory systems and compliance issues with software utilization.

Key Findings

The DMV is not routinely completing an annual risk assessment of its information systems and does not have monitoring controls in place. Additionally, the DMV does not have fully documented plans related to critical IT operations and functions and did not follow the documented plans they do have when issues arose. (page 4)

There is no process or policy to track and monitor hard drives from receipt to disposal to ensure devices are thoroughly cleaned or destroyed when the hard drive is retired. In addition, hard drives in leased equipment may not be recovered and data destroyed since the DMV does not have an effective process to collect hard drives before equipment is removed from the premises. (page 5)

During our review of the systems patch management process, we found servers, computers, and other devices that were not receiving updates consistently. By not updating these devices routinely, the DMV is increasing the potential for a data breach or malware infection. (page 7)

The DMV does not have a change management procedure with which to track the request, approval, and implementation of hardware changes. During our review of the DMV's change management process, IT staff were unable to provide documentation of any kind related to the configuration of 25 selected devices which included servers, computers, and switches. (page 8)

The DMV does not monitor data extractions performed for third-party entities or review logs for changes to sensitive information. Consequently, we could not determine if information provided to third parties was appropriate and matched original data requests. (page 8)

User access management is weak for DMV systems. Specifically, the DMV's user access management and ITSEC form process should be timelier and more accurate. Additionally, the DMV is not reviewing user access regularly, including local administrator permissions, or ensuring that user accounts with domain administrator rights are not used for daily operations such as internet browsing, email, or similar activities. (page 11)

The DMV's ITSEC forms lack approved access consistency. The two top-level primary application users have full access to the application; however, the ITSEC forms do not reflect their administrative access or their updated positions. Additionally, the DMV does not ensure permissions for routine positions are appropriate. (page 12)

The DMV did not consistently remove former or inactive employees' network access in a timely manner. Additionally, third-party users with significant periods of inactivity were not monitored or reviewed for the need for continued access. (page 13)

The DMV's computer hardware management process can be improved. Our review found the DMV's asset inventory is not accurate, showing IT assets missing from inventory records and other discrepancies between internal listings and state inventory records. In addition, the DMV does not currently have a software reconciliation policy and software is not included in the DMV's annual inventory process. (page 14)

For more information about this or other Legislative Auditor reports go to: http://www.leg.state.nv.us/audit (775) 684-6815.

Audit Division
Legislative Counsel Bureau