LA24-08

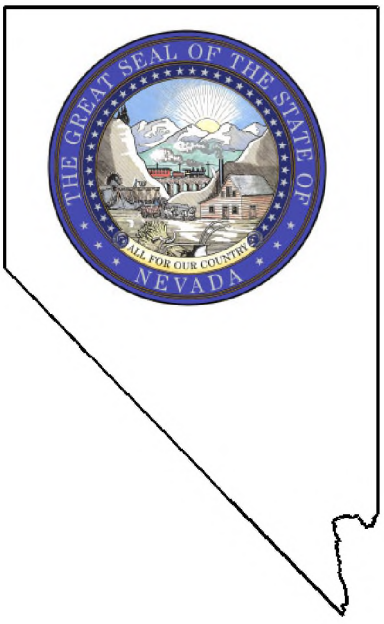
STATE OF NEVADA

Performance Audit

Department of Motor Vehicles

Information Security

2023



Legislative Auditor
Carson City, Nevada

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

STATE OF NEVADA

LEGISLATIVE COUNSEL BUREAU

CARSON CITY OFFICE
LEGISLATIVE BUILDING
401 S. CARSON STREET
CARSON CITY, NEVADA 89701
(775) 684-6800

LAS VEGAS OFFICE
GRANT SAWYER STATE OFFICE BUILDING
555 E. WASHINGTON AVENUE, SUITE 4400
LAS VEGAS, NEVADA 89101
(702) 486-2800

Legislative Commission
Legislative Building
Carson City, Nevada

This report contains the findings, conclusions, and recommendations from our performance audit of the Department of Motor Vehicles (DMV), Information Security. This audit was conducted pursuant to the ongoing program of the Legislative Auditor as authorized by the Legislative Commission. The purpose of legislative audits is to improve state government by providing the Legislature, state officials, and Nevada citizens with independent and reliable information about the operations of state agencies, programs, activities, and functions.

This report includes 17 recommendations to improve the security of the DMV's information systems. We are available to discuss these recommendations or any other items in the report with any legislative committees, individual legislators, or other state officials.

Respectfully submitted,

Daniel L. Crossman, CPA
Legislative Auditor

August 7, 2023
Carson City, Nevada

Department of Motor Vehicles Information Security

Table of Contents

Introduction

Background

The Department of Motor Vehicles (DMV) was founded in 1957 to administer driver licensing and motor vehicle laws. The mission of the 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 currently licenses 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. In addition, the DMV helps ensure highway safety through:

- Testing and driver education;
- Administering financial responsibility laws and licenses;
- Regulating the vehicle industry, including car dealers, salespeople, rental car companies, manufacturers, emissions inspection stations, and private driving schools and instructors; and
- Investigating identity theft, vehicle fraud, and consumer complaints.

Approximately 10 million transactions are processed and $1.6 billion in revenue is collected at the DMV each year. This includes fuel taxes and governmental services taxes to help fund local governments and schools.

The DMV has seven divisions, including Field Services, Research and Project Management, Administrative Services, Motor Carrier, Central Services and Records, Compliance Enforcement, and Motor Vehicle Information Technology (MVIT). There are 5 metropolitan and 11 rural office locations throughout Nevada. DMV operates with more than 1,100 employees of which about 65

are dedicated to information technology functions. As of April 2023, DMV's vacancy rate approached nearly 12%. Exhibit 1 shows DMV's positions and vacancies by budget account.

Positions and Vacancies by Budget Account **Exhibit 1**
April 2023

Budget Accounts	Authorized Positions	Filled Positions	Vacant Positions
Records Search	15	12	3
License Plate Factory	6	5	1
Automation	80	65	15
System Modernization	29	27	2
Motor Carrier	51	41	10
Motor Vehicle Pollution Control	37	33	4
Verification of Insurance	21	14	7
Hearings	11	10	1
Field Services	745	678	67
Compliance Enforcement	82	71	11
Central Services	131	105	26
Management Services	16	16	0
Director's Office	19	19	0
Administrative Services	53	47	6
Totals	**1,296**	**1,143**	**153**

Source: Human Resource Data Warehouse.

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.

Scope and Objective

The scope of our audit covered the information systems and related practices in place during fiscal years 2022 and 2023. We also reviewed information back to 2020 for user access and 2021 for asset inventory. Our audit objective was to:

- Determine if the DMV has adequate information security controls in place to protect its information processing systems.

This audit is part of the ongoing program of the Legislative Auditor as authorized by the Legislative Commission and was made

pursuant to the provisions of Nevada Revised Statutes (NRS) 218G.010 to 218G.350. The Legislative Auditor conducts audits as part of the Legislature's oversight responsibility for public programs. The purpose of legislative audits is to improve state government by providing the Legislature, state officials, and Nevada citizens with independent and reliable information about the operations of state agencies, programs, activities, and functions.

Essential Information Technology Functions Need Additional Oversight

The DMV has not 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, the DMV's data is vulnerable since the data destruction and patch management processes do not track or monitor hardware needing data sanitization or necessary software updates. Adequate IT policies protect entities from unnecessary security exposure and prolonged system failure recovery.

Annual Risk Assessment and Policies Not Completed

The DMV is not routinely completing an annual risk assessment of its information systems. The last risk assessment was completed in 2019. Additionally, the DMV is not routinely evaluating existing controls and policies. These issues occurred because the DMV does not have monitoring controls to ensure significant IT-related activities occur in frequency with established standards.

Reviewing risks and established policies annually does the following:

- Identifies new vulnerabilities so controls can be developed and implemented to mitigate identified risks; and
- Ensures existing controls and policies operate as intended; thereby, managing security risks and exposure within IT systems.

State security policy requires state agencies to conduct a self-risk assessment of their information security controls at least annually and revise their controls according to identified inadequacies or new risks.

Critical Plans Incomplete or Not Followed

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. Specifically, the DMV does not have continuity of operations or disaster recovery plans that can be used to minimize the effects of a major failure of information systems, counteract interruptions to business activities, and protect critical business processes at the DMV. Planning for contingencies related to IT functions is critical for agencies to mitigate disruptions and guide staff in restoring services and functionality during crisis events.

Additionally, the DMV's incident response plan (IRP) was in draft form and not fully implemented. One incident occurred during the audit which resulted in one of the DMV's user portals being down for over 10 hours. While the DMV's response was appropriate, the IRP was not followed. Following a documented IRP helps ensure issues do not compound and the restoration of services is not delayed.

State security policies require agencies to define and implement appropriate processes and develop plans to ensure the reasonable and timely recovery of all state agency information, applications, systems, and security regardless of the computing platform. Plans were not developed and properly implemented because the DMV relied solely on one individual to develop IT-related plans and activities. Well developed internal control systems plan for personnel contingencies through training and succession planning.

No Tracking or Monitoring of Data Destruction

The DMV's data destruction process is insufficient. Specifically, the DMV does not have processes or policies to track and monitor hard drives from receipt to disposal, to ensure devices are thoroughly cleaned or destroyed when the hard drive is retired. Additionally, the 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 IT equipment is removed from the premises. Effective data destruction processes are important to ensure sensitive information is not compromised.

During our review of the DMV's hard drive destruction process, we encountered several boxes filled with hard drives that were not labeled but were awaiting destruction. Exhibit 2 shows an example of untracked hard drives.

Untracked Hard Drives **Exhibit 2**

Box of hard drives in IT office with no indication of origin, data classification, or destruction status.

Source: Picture taken by auditor, Carson City DMV.

State security standards require methods to be developed and documented to ensure sanitization and disposal of media are commensurate with the sensitivity and criticality of the data residing on the storage devices, equipment, and hardcopy. In addition, vendor contracts indicate that multi-functional devices (MFD) storage components (hard drives) must be left in the possession of the DMV before an MFD is removed.

The process for recovering hardware from MFD's differs from other IT related assets since the physical asset is taken back by the lessor. As such, it is vital the DMV has a well defined and

executed process for removing drives before the asset leaves the premises, to ensure sensitive data is not compromised. The DMV IT division does not log or track the hardware as it is received, when the data is erased, or when the hardware is recycled. As a result, the DMV cannot reasonably ensure that sensitive data is properly secured and appropriately destroyed before devices leave state custody. Because hard drives can contain personally identifiable information (PII), adequate controls and policies are necessary to protect citizens and the State from harm.

Patch and Change Management Needs Improvement

The DMV's security patching and change management processes lack oversight, consistency, and documentation. In addition, the DMV does not have a documented procedure for tracking the request, approval, implementation, and documentation of hardware configuration changes made to its information systems. Issues can occur when assets do not receive current updates or changes made to devices have not been approved.

Patch Management

During our review of the systems patch management process, we found some virtual servers, physical servers, desktop computers, laptop computers, and MFDs that were not receiving updates consistently. By not updating these devices routinely, the DMV is increasing the potential for a data breach and or malware infection. The DMV uses an email reminder for system patches sent out to administrators; however, no follow up occurs to ensure the completion of the process. Furthermore, there is no schedule or reminder emails in place to ensure MFDs or other IT assets are receiving current updates.

Additionally, approval for applying patches was not always documented. Of the 46 patches tested, 11 (24%) were missing approval. Without an effective patch management approval process, the DMV increases the potential that patches could affect the functionality and reliability of the primary IT application. The approval email process is not documented and lacks oversight from the beginning of the process to the patch implementation.

The DMV is responsible for creating a consistent maintenance window not less than semimonthly for the deployment of software

updates and patches. The DMV is also responsible for deploying and using automated software update tools on technology assets and networks. This ensures that agency assets are running the most recent security updates provided by the software vendor for all software, to maximize protection against security vulnerabilities and minimize the impact on agency business operations. Lastly, the DMV is responsible for following its internal process of approving patches for the primary DMV application.

Change Management

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. The DMV does not have a change management procedure to track the request, approval, and implementation of hardware changes. Without an effective change management procedure, the DMV cannot track all hardware configuration changes made in their IT environment, which could result in prolonged network or systems interruptions.

State security standards require all agencies to establish, implement, and maintain documented security configuration standards for all authorized systems and network hardware. This includes procedures for the request, approval, implementation, and documentation of all hardware configuration changes.

Limited Documentation Over Data Sales

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.

Data is sold to outside entities in accordance with NRS 481.063 and Nevada Administrative Code 481.500 – 481.600. Data includes personal information such as the names and mailing address of citizens. However, law does not allow for certain sensitive information such as specific driver's license or registration information to be sold to third parties. Sales of data to outside entities have occurred for many years and documentation approving the nature and extent of information provided is no longer maintained by the DMV. Since documentation detailing the

nature of the information requested is not available, it is impossible to know if the data extracted and provided to outside entities was proper. We requested documentation for two extraction jobs and no documentation could be provided supporting the nature and content of the information being sold.

The DMV has an established process for data sales; however, the application, approval, and data extraction processes are performed by two separate divisions. Once the data extraction is set up, the DMV does not retain documentation detailing the nature, reason, and approval for providing the information even though data continues to be provided to these outside entities.

Poor documentation around data sales puts the DMV's sensitive data at risk. It makes it difficult to verify the data being sold is authorized and approved. In addition, the ability to control who has access to potentially sensitive information is decreased.

Personally Identifiable Information Modifications Not Reviewed

Modifications to PII within DMV records are not always reviewed. Six of the 67 programmer-initiated Social Security Number (SSN) modifications tested did not contain any reason for why the SSN was accessed or changed in the application. The DMV uses an audit program to track all modifications to SSNs; however, a reason is not required to be entered for the change to occur. Furthermore, the DMV does not have a policy or process in place to review sensitive data access logs.

The potential risk associated with unauthorized or unintentional modification of DMV customer personal information could result in identity theft or fraud. Modifications were allowed without a reason because logs are not reviewed by management; therefore, the issue was not identified.

State security standards require all state agencies protect sensitive information from unauthorized or unintentional disclosure or modification and require logs to be analyzed to identify unauthorized activity.

Recommendations

1. Develop a review and approval process to ensure an information systems risk assessment is completed at least annually.
2. Prioritize the development of disaster recovery and continuity of operations plans and a documented testing schedule.
3. Ensure the state security policies are being reviewed and implemented by those responsible.
4. Cross-train and delegate functions to ensure vital information technology processes and plans are followed and completed.
5. Update the DMV's data destruction policy to include procedures for hard drive collection, tracking, and data destruction verification.
6. Develop policies and procedures to ensure patches are approved and installed routinely and timely, including periodic monitoring of all devices to ensure the most recent software patches have been applied.
7. Properly review patching reports and require updates to be applied, as necessary.
8. Develop, document, and follow a security configuration and change management procedure for DMV's information systems.
9. Document the process for the sale of DMV's data to include monitoring and review controls and ensure proper retention of related documentation.
10. Assess and document appropriate log review procedures for Social Security Number modifications in the DMV's primary application.

Better Controls Over Access to Systems Needed

The DMV has not fully implemented controls over employee 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.

Employee User Access Needs Greater Review

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.

DMV information technology staff utilize ITSEC forms to establish and revoke user access to systems. Since DMV's primary method of modifying user access is through an ITSEC form, completion of this process by user supervisors is important for communicating changes needed. However, our review found 10 of 15 terminated DMV users tested did not have an updated ITSEC form indicating their termination status. In addition, one of three non-DMV users who had been terminated did not have updated ITSEC forms. At the time of our testing, users were separated from service for 109 days on average without updated forms being completed and processed.

Furthermore, forms were not always updated when necessary or relevant information was needed to ensure access provided was appropriate. Our review of 15 ITSEC forms showed forms did not specify the access rights provided to the user.

The DMV recently implemented a new digital ITSEC form request system which replaced the outdated manual form process. At the time of the audit, the new digital process had not been fully implemented and staff had not been trained on it. Additionally, the DMV has not established a plan for integrating existing ITSEC forms into the digital system or ensuring quarterly reviews, which could lead to security issues.

Inconsistent Accessibility

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. Furthermore, 4 of 11 users tested were able to download and install unauthorized software without elevated permissions. Two of those users were motor vehicles information technology administrators who use this account for daily activities, which increases the risk that attackers could gain access to those credentials.

Additionally, the DMV does not ensure permissions for routine positions are appropriate. For instance, we found multiple variations in user access profiles for the same position. For the 11 forms reviewed, none indicated why some users were provided access to additional modules and functions in the software system than others.

The DMV does not review all user profiles quarterly as required by state security standards and does not have procedures regarding the assignment, review, and documentation of user profiles. This increases the risk that intruders could gain access to DMV systems, move around the network, access applications undetected, and lead to other security issues.

State security standards require all agencies to ensure users with administrative accounts use a dedicated or secondary account for

elevated activities. These accounts are not intended for internet browsing, email, or similar activities.

User Accounts Were Not Updated Timely

Because ITSEC forms are not completed timely and routine reviews of user accounts do not occur, 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. Monitoring and reviewing user access is important because DMV applications contain sensitive data and information that could be exploited.

We found:

- 15 terminated users had active application accounts;
- 6 third-party users had inactivity exceeding 3 months, of which, two were terminated upon our request for information;
- 11 of 14 users had position changes that were not updated on their ITSEC forms; and
- 66 active primary application accounts belonged to terminated DMV employees.

Users were not removed timely because the DMV does not have a process in place to ensure that all users, both system and application, are reviewed quarterly to ensure accounts are updated. Therefore, the DMV cannot reasonably ensure that unauthorized access does not occur.

State security standards dictate that information technology systems and networks must have logical access controls to protect them from unauthorized access, alteration, loss, disclosure, and availability of information. In addition, user accounts must be reviewed quarterly to ensure the continued need for access to a system and that transferred or reassigned users have been deleted. Further, system managers shall reevaluate system access privileges granted to all users quarterly, at a minimum.

Inventory Controls Inadequate

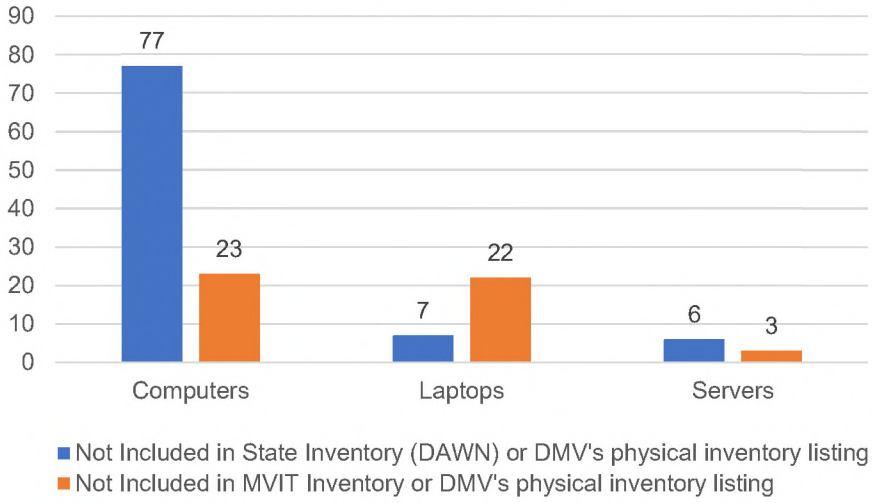
The DMV's inventory controls are inadequate over IT assets. The computer hardware inventory process does not include reconciliation from one inventory system to another to verify assets connected to the network are verified and appropriate. In addition, the DMV has not yet implemented a computer software inventory process which puts them out of compliance with state security standards.

Information Technology Assets Not Monitored

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. This occurred because the DMV does not reconcile IT assets across systems.

The DMV has an asset management software system that monitors IT assets on its network. This software shows IT equipment utilizing the network and is beneficial for identifying unauthorized devices accessing its systems. However, the DMV does not reconcile this system with its official state inventory resulting in discrepancies across desktop and laptop computers and servers as seen in Exhibit 3.

Inventory Records Comparison August 2022 **Exhibit 3**



Source: Auditor prepared from test results and DMV inventory records.

Because the DMV does not perform inventory reconciliations, hardware with sensitive data could be lost or stolen. In addition, unauthorized IT assets using the network would not be detected in a timely manner, or at all, and could put the State at risk.

State security standards require a physical inventory review and reconciliation of all state property, including detailed hardware asset inventory of all technology assets with the potential to store or process information whether connected to the network or not.

Software Used in Excess of Licenses

The DMV does not currently have a software reconciliation policy and software is not included in the DMV's annual inventory process. During our review, we found that one software license assessed was installed 42 times over the purchased limit. The DMV is in the process of developing a software inventory user guide and policy; however, it had not completed or implemented this process during our audit.

Not managing software in an enterprise environment creates the increased risk of unnecessary recurring purchases, the potential of paying license fees or maintenance fees for assets that do not exist, and high costs and consequences of using software in excess.

State security standards require the establishment of monitoring controls for software compliance. In addition, the DMV should follow its internal policy which includes inventory review and reconciliation to ensure adequacy.

Recommendations

11. Document and train DMV's staff on the new digital Information Technology Security form process and follow procedures to ensure no access or permissions are added, modified, or disabled without an Information Technology Security form.
12. Remove unnecessary local administrator permissions from DMV's devices.

13. Create dedicated system administrator user accounts for all elevated system administrator activities.
14. Develop a quarterly review process to ensure access and permissions in DMV's systems are appropriate and authorized, and that the Information Technology Security forms reflect those approved permissions.
15. Enhance the DMV's information technology equipment inventory policy to include a reconciliation based on the annual physical inventory for equipment across DMV's asset management system and other inventory tracking reports. Update all systems for information technology equipment additions and deletions.
16. Complete the software inventory user guide and develop policies and controls to detect software licenses installed in excess of those purchased.
17. Perform software compliance analysis and determine whether any liability exists associated with software licenses utilized exceeding the number purchased.

Appendix A
Audit Methodology

To gain an understanding of the Department of Motor Vehicles (DMV) information security controls, we interviewed management and motor vehicle information technology (MVIT) personnel. Through discussions and documentation review, we gained a broad understanding of how DMV information security is managed. In addition, we reviewed state security policies, standards, procedures, laws, and administrative codes. We also reviewed the DMV's policies, financial information, budgets, and other information describing the DMV's activities. Furthermore, we documented and assessed internal controls over information technology policies, data destruction and security processes, access control, and asset management.

Our audit included a review of the DMV's internal controls significant to our audit objective. Internal control is a process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved. Internal control comprises the plans, methods, policies, and procedures used to fulfill the mission, strategic plan, goals, and objectives of the entity. The scope of our work on controls included the following:

- Exercise oversight responsibility; establish structure, responsibility, and authority; evaluate performance and enforce accountability (Control Environment);
- Define objectives and risk tolerances; and identify, analyze, and respond to change (Risk Assessment);
- Design control activities; implement control activities through policy (Control Activities);

- Communicate internally (Information and Communication); and

- Perform monitoring activities; evaluate issues and remediate deficiencies (Monitoring).

Deficiencies and related recommendations to strengthen the DMV's internal control systems are discussed in the body of the report. The design, implementation, and ongoing compliance with internal controls are the responsibility of agency management.

To assess the overall risk posture of the DMV, we requested and reviewed their current information security documentation, including their security risk assessment, disaster recovery, incident response, and continuity of operations plans. In addition, we had discussions with DMV staff regarding the DMV's compliance with state security standards, policies, and procedures.

To confirm satisfactory data destruction practices, we selected devices that were replaced or removed to ensure that the hard drives associated were wiped or destroyed following the DMV's standard procedures and state-specified security standards. In addition, we observed the data sanitation process and reviewed contractual agreements with multi-functional device (MFD) lessors to determine if adequate data destruction practices are followed.

We also analyzed the patch management process of the DMV's primary application by determining the extent of management oversight and approval based on management interviews and documentation supporting management review. We randomly selected 20 computer devices, a little over 1% of the population, and judgmentally selected 7 MFD's, 29% of the population, to determine if updates were applied properly and timely.

We inspected change management for devices added to the DMV network by judgmentally selecting the five most recently added devices from each of the following asset categories: virtual and physical servers, laptop and desktop computers, vendor devices, and switches for just under 1% of the population. For each of our selections, we determined whether the devices were added by

following the DMV's standard policies and procedures, as well as security standards.

To evaluate the adequacy of the sale of data to third parties, we assessed the completeness of the reviewed available information regarding data extractions and documentation supporting this process. Furthermore, we tested all Social Security Number modifications by reviewing logs and determining if all searches were adequately recorded and the reason for the modification identified.

To determine if user access management was appropriate, we reconciled the user lists from the DMV's systems and the state human resources system. We judgmentally selected 44 primary application users, about 9% of the population, to test actual and authorized access rights. Our testing included new, modified, and terminated users. We utilized DMV user selections and the user listings provided by the DMV to identify instances where access rights and privileges appear unnecessary. In addition, we requested verification that quarterly user access reviews were being conducted. Lastly, we judgmentally selected 11 Service Technician 1 users, about 5.5% of the population, with similar roles to determine if they had consistent profiles.

To test the DMV's computer system asset management process, we reviewed the policies and procedures surrounding hardware and software inventory. We tested the hardware asset inventory by reconciling the state inventory system, the MVIT computer inventory system, and the DMV's previous annual inventory data. The DMV's annual inventory listing included 1814 devices which included 1211 computers, 55 servers, and 548 laptops. We verified the software asset inventory by comparing licenses purchased with licenses installed on devices.

We used nonstatistical audit sampling for our audit work, which was the most appropriate and cost-effective for concluding on our audit objective. Based on our professional judgment, review of authoritative sampling guidance, and careful consideration of underlying statistical concepts, we believe that nonstatistical sampling provided sufficient, appropriate audit evidence to support

the conclusions in our report. We did not project exceptions to the population because our samples were selected judgmentally, which does not lend itself to projecting the population.

Our audit work was conducted from February 2022 to January 2023. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

In accordance with NRS 218G.230, we furnished a copy of our preliminary report to the Director of the Department of Motor Vehicles. On July 26, 2023, we met with agency officials to discuss the results of the audit and requested a written response to the preliminary report. That response is contained in Appendix B, which begins on page 21.

Contributors to this report included:

Christopher Gray, MPA
Deputy Legislative Auditor

Adam Prohoroff, CIA, CISA, CPA
Deputy Legislative Auditor

Shirlee Eitel-Bingham, CISA
Information Security, Audit Manager

Shannon Riedel, CPA
Chief Deputy Legislative Auditor

Appendix B

Response From the Department of Motor Vehicles

Joe Lombardo
Governor

Julie Butler
Director

Tonya Laney
Deputy Director

555 Wright Way
Carson City, Nevada 89711
Telephone (775) 684-4368
dmv.nv.gov

August 3, 2023

Daniel L. Crossman, CPA, Legislative Auditor
Legislative Counsel Bureau, Audit Division
401 S. Carson Street
Carson City, NV 89701-4747

Dear Mr. Crossman:

Enclosed please find the Department of Motor Vehicles' response to the Legislative Auditor's preliminary audit report on the DMV's Information Security. The Department has accepted all seventeen recommendations and is actively working on remediating the deficiencies that were noted in the report.

Sincerely,

Julie Butler

Julie Butler, Director
Department of Motor Vehicles

LCB Security Audit Findings & Remediation Plan Summary

1. **Develop a review and approval process to ensure an information systems risk assessment is completed at least annually.**

   Answer: DMV is currently formalizing an internal certification and accreditation process that governs system risk assessments and authorizations. This process is documented in the DMV System Security Plan and ensures adherence to State Security Policy and Standards. The Department will be requesting a new full-time position to manage Internal and External Audit functions to support agency Certification and Accreditation activities and internal assessments as an agency role moving forward.

2. **Prioritize the Development of Disaster Recovery and Continuity of Operations Plans and documented testing schedule.**

   Answer: DMV ISOs have documented Disaster Recovery and Continuity of Operations Plans and documented testing schedules. The DMV tabletop COOP and Incident Response Plan (IRP) tabletop scenario exercises will be completed in Q4/FY23.

3. **Ensure the State Security Policies are being reviewed and implemented.**

   Answer: DMV ISOs are actively performing risk assessments for the DMV Transformation Effort (DTE) and the DMV Legacy System (CARRS). DMV Security Policies and Security Plans have been updated. All Security Policies are under routine ISO review.

4. **Cross-train and delegate functions to ensure vital information technology processes and plans are followed and completed.**

   Answer: DMV ISOs have documented COOP, DR, and Incident Response Plans. COOP, DR, and Incident Response tabletop exercises are currently being planned and will take place in Q4/FY23. DMV ISOs have developed and implemented a Security & Privacy Portal that is shared with all staff for security policy awareness, socialization, and transparency.

5. **Update the DMV's data destruction policy to include procedures for hard drive collection, tracking, and data destruction verification.**

   Answer: The DMV Data Destruction policy has been updated to reflect adherence to state security standards and NIST guidelines. This has been communicated and socialized with desktop support, who worked with our ISOs in a collaborative effort for this purpose.

6. **Develop policies and procedures to ensure patches are approved and installed routinely and timely, including periodic monitoring of all devices to ensure the most recent software patches have been applied.**

   Answer: The DMV Patch Management Policy, MVIT – 20, is in the process of being updated and enhanced. ISOs are increasing oversight and communications to responsible patching groups with discussions underway around timely and efficient patch management. ISOs are monitoring patch compliance utilizing Altiris and Tenable Security Center for vulnerability management. The potential for a dedicated FTE patch person is being considered.

7. **Properly review patching reports and require updates to be applied, as necessary.**

   Answer: DMV is utilizing tools such as Altiris and Tenable Security Center for vulnerability and patch management. All ISOs now have access for increased oversight and to verify patch status and compliance. ISOs communicate to responsible groups for patch management remediation. DMV ISOs have documented security policy within the DMV Security and Privacy Portal related to patch management, vulnerability monitoring, and scanning. Per this policy, when vulnerabilities are discovered, they must be mitigated within a given timeframe. The potential for a dedicated FTE patch person is being considered.

8. **Develop, document, and follow a security configuration and change management procedure for DMV's information systems.**

   Answer: DMV ISOs have documented security controls and standards related to configuration management within the DMV Security and Privacy Portal. ISOs have identified existing policies and processes for standardized secure configuration of devices and software and have these currently under review for enhancement. DMV is considering utilizing the Center for Internet Security (CIS) hardened images, which the state has a blanket license for as MS-ISAC members. Reference CIS implementation groups (IG version 7+) as required by state standard. CIS Cat pro may be used as an audit tool for secure configuration and to further enhance secure standard images and configuration. This can be used for servers and workstations of all operating system versions. ISOs are working with MVIT management and staff members to streamline and further develop the processes and documentation.

9. **Document the process for the sale of DMV's data to include monitoring and review controls and ensure proper retention of related documentation.**

   Answer: DMV ISOs have documented the DMV Data Governance and Privacy Program. This program ensures DMV oversight for data exchanges with external partners and provides evaluation of:

   - Privacy Impact Assessment of data transmitted and exchanged externally to DMV partners and customers.

- Establishes an annual Privacy Risk Assessment intended to conduct organizational data privacy risk assessments that consider the entire life cycles of all business processes that involve collecting, using, maintaining, sharing, or disposing of PII.
- Assess Privacy Security Controls associated with Data Governance activities within the DMV and form the baseline standard for an organizational Data Governance Analysis and Privacy Impact Assessments.
- The Department will be asking for an FTE to manage Data Governance Activities as an agency role.

10. **Assess and document appropriate log review procedures for Social Security Number modifications in the DMV's primary application.**

    Answer: DMV ISOs are working on implementing a process for tracking and monitoring batch pulls for information and requiring SolarWinds Service Desk tickets for SQL Audits. DMV ISOs have documented audit log related security control policies.

11. **Document and train DMV's staff on the new digital Information Technology Security form process and follow procedures to ensure no access or permissions are added, modified, or disabled without an Information Technology Security form.**

    Answer: DMV is currently reviewing and updating policy to ensure no access or permissions are added, modified, or disabled without an Information Technology Security form. We are performing reviews of vendors and 3rd party access quarterly and identifying and disabling inactive accounts. We are now utilizing ManageEngine for Active Directory audits, looking at last 90-day activity, flagging accounts to be disabled if no activity, and disabling after 30 days.

12. **Remove unnecessary local administrator permissions from DMV's devices.**

    Answer: We are performing quarterly Active Directory and CARRS user audits, including auditing of active and non-active accounts and associated permissions. We are developing policy for performing these audits and the potential changes needed which are identified. Tracking of the audits and changes performed with an associated IT Sec form which will also be part of the audit, and possibly be included in SolarWinds Service Desk. We are now using ManageEngine to perform audits against Active Directory, which may include automated alerts and reports for continuous monitoring.

13. **Create dedicated system administrator user accounts for all elevated system administrator activities.**

    - Answer: DMV ISOs and MVIT are reviewing GPO settings and roles for the DMV domain. We are now using ManageEngine to perform audits against Active Directory. We are performing quarterly Active Directory and CARRS user audits, including auditing of active and non-active accounts and associated permissions. We are developing a policy for performing these audits and the potential changes needed.

14. **Develop a quarterly review process to ensure access and permissions in DMV's systems are appropriate and authorized, and that the Information Technology Security forms reflect those approved permissions.**

    Answer: We are performing quarterly Active Directory and CARRS user audits, including auditing of active and non-active accounts and associated permissions. We are developing a policy for performing these audits and the potential changes needed. Tracking of the audits and changes performed with an associated IT Sec form which will also be part of the audit and may be included in SolarWinds Service Desk.

15. **Enhance the DMV's information technology equipment inventory policy to include a reconciliation based on the annual physical inventory for equipment across DMV's asset management system and other inventory tracking reports. Update all systems for information technology equipment additions and deletions.**

    Answer: We are updating the DMV's information technology equipment inventory policy to include a reconciliation based on the annual physical inventory. This will include a request of a current Property Disposition Report from State Purchasing for a list of devices that have been removed or changed.

16. **Complete the software inventory user guide and develop policies and controls to detect software licenses installed in excess of those purchased.**

    Answer: Policy enhancements are needed and are underway. We are working to complete the software inventory user guide and further develop related policy, while identifying technical solutions to assist in the process.

17. **Perform software compliance analysis and determine whether any liability exists associated with software licenses utilized exceeding the number purchased totals.**

    Answer: We are working to complete and reconcile inventory periodically with the list from State Purchasing and DAWN on a set schedule, and fine-tuning software license tracking and detection method(s) for exceeding them and compensating controls. ISOs and MVIT are discussing additional tracking methods with the various DMV divisions.

Department of Motor Vehicles' Response to Audit Recommendations

	Recommendations	Accepted	Rejected
1.	Develop a review and approval process to ensure an information systems risk assessment is completed at least annually	X	
2.	Prioritize the development of disaster recovery and continuity of operations plans and a documented testing schedule	X	
3.	Ensure the state security policies are being reviewed and implemented by those responsible	X	
4.	Cross-train and delegate functions to ensure vital information technology processes and plans are followed and completed	X	
5.	Update the DMV's data destruction policy to include procedures for hard drive collection, tracking, and data destruction verification	X	
6.	Develop policies and procedures to ensure patches are approved and installed routinely and timely, including periodic monitoring of all devices to ensure the most recent software patches have been applied	X	
7	Properly review patching reports and require updates to be applied, as necessary	X	
8.	Develop, document, and follow a security configuration and change management procedure for DMV's information systems	X	
9.	Document the process for the sale of DMV's data to include monitoring and review controls and ensure proper retention of related documentation	X	
10.	Assess and document appropriate log review procedures for Social Security Number modifications in the DMV's primary application	X	
11.	Document and train DMV's staff on the new digital Information Technology Security form process and follow procedures to ensure no access or permissions are added, modified, or disabled without an Information Technology Security form	X	
12.	Remove unnecessary local administrator permissions from DMV's devices	X	
13.	Create dedicated system administrator user accounts for all elevated system administrator activities	X	

Department of Motor Vehicles' Response to Audit Recommendations (continued)

	Recommendations	Accepted	Rejected
14.	Develop a quarterly review process to ensure access and permissions in DMV's systems are appropriate and authorized, and that the Information Technology Security forms reflect those approved permissions	X	
15.	Enhance the DMV's information technology equipment inventory policy to include a reconciliation based on the annual physical inventory for equipment across DMV's asset management system and other inventory tracking reports. Update all systems for information technology equipment additions and deletions	X	
16.	Complete the software inventory user guide and develop policies and controls to detect software licenses installed in excess of those purchased	X	
17.	Perform software compliance analysis and determine whether any liability exists associated with software licenses utilized exceeding the number purchased	X	
	TOTALS	17	