LA26-07

STATE OF NEVADA

Performance Audit

Multi-Agency Information Security

Division of Public and Behavioral Health
Office of the Secretary of State
Cannabis Compliance Board
Employment Security Division

2025

Legislative Auditor
Legislative Counsel Bureau – Audit Division

Audit Highlights

Highlights of performance audit report on Multi-Agency, Information Security, the Division of Public and Behavioral Health, the Office of the Secretary of State, the Cannabis Compliance Board, and the Employment Security Division issued on April 15, 2026.

Legislative Auditor report # LA26-07.

Background

The Division of Public and Behavioral Health's (DPBH) mission is to protect, promote, and improve the physical and behavioral health of the people of Nevada. DPBH is part of the Department of Health and Human Services.

The Nevada Secretary of State is elected to a 4-year term and is responsible for maintaining the official records of the acts of the Nevada Legislature and the Executive Branch of State Government.

The Cannabis Compliance Board (CCB) consists of five Governor appointed board members. The CCB governs Nevada's cannabis industry through strict regulation of all areas of its licensing and operations, protecting the public health and safety of citizens and visitors while holding cannabis licensees to the highest ethical standards.

The Employment Security Division (ESD) has a vision of creating success for businesses and Nevadans. ESD exists to empower a vibrant labor market in Nevada by creating business and worker connections with high-quality, demand-driven services. ESD is a division of the Department of Employment, Training and Rehabilitation.

Purpose of Audit

The purpose of the audit was to determine if the selected agencies have adequate information security controls in place over risk assessment, asset inventory, vulnerability management, and security awareness training to ensure the protection of information technology systems and the data those systems process, store, and transmit. This audit included the systems and practices in place during calendar years 2023 and 2024.

Audit Recommendations

This audit report contains 27 recommendations to improve information security controls across 4 agencies.

The Division of Public and Behavioral Health accepted the seven applicable recommendations. The Office of the Secretary of State accepted the seven applicable recommendations. The Cannabis Compliance Board accepted the six applicable recommendations. The Employment Security Division accepted the seven applicable recommendations.

Recommendation Status

Each agency's 60-day plan for corrective action is due on July 11, 2026. In addition, the 6-month report on the status of audit recommendations is due on January 11, 2027.

Multi-Agency Information Security

Division of Public and Behavioral Health (DPBH)

Summary: Information system controls at DPBH need improvement to strengthen security, efficiency, and oversight of their operating information technology (IT) environment. Weaknesses identified include: DPBH has not completed a risk assessment of the full operating IT environment, the inventory and control of enterprise assets does not include a physical inventory of assets, the continuous vulnerability management program lacks documented procedures, and the security awareness training program lacks internal policies and procedures.

Key Findings: DPBH has not conducted and documented a security risk assessment or an annual security controls self-assessment as required by state standards. (page 5) DPBH does not conduct a physical inventory of IT assets. (page 7) DPBH does not have a policy or process in place to track how long a vulnerability has been active nor do they have the ability to identify what vulnerabilities are being worked on or remediated. (page 9) DPBH utilizes the State's enterprise-managed security awareness training and simulated phishing platform as their primary cybersecurity training tool; however, the agency does not have any internal policies specific to security awareness training. (page 11)

Office of the Secretary of State (SOS)

Summary: Information system controls at SOS need improvement to strengthen security and improve oversight of the operating IT environment. Weaknesses identified include: a documented full risk assessment or annual self-assessment of information security controls has not occurred, the inventory and control of enterprise assets lack consistency and completeness, the continuous vulnerability management program lacks documentation and remediation processes, and the security awareness training program does not ensure all employees are completing their initial and annual training.

Key Findings: SOS has not completed a documented full risk assessment or prepared an annual self-assessment of information security controls. (page 14) SOS conducts semi-formal annual inventory procedures; however, there are no documented procedures for conducting the annual inventory and pertinent information is missing. (page 15) SOS lacks documented procedures for maintaining its vulnerability management program and tracking of vulnerabilities found in the operating IT environment. (page 16) SOS utilizes the State's enterprise-managed security awareness training and simulated phishing platform as its primary cybersecurity training tool. All 129 agency employees were properly enrolled in the security awareness training program and required to complete their annual training or initial security awareness training within the first 90 days of employment as required by state policy. However, training was not always completed on time. (page 18)

Cannabis Compliance Board (CCB)

Summary: Information system controls at CCB need improvement as there is a lack of documented policies and procedures. Weaknesses identified include: a full information security risk assessment has not occurred, the inventory and control of enterprise IT assets process does not follow CCB policy, the continuous vulnerability management program is not fully implemented, and the security awareness training program needs improvement.

Key Findings: CCB has been active for over 4 years and has not conducted and documented a full information security risk assessment. (page 21) While CCB is conducting an annual inventory of assets, they are not updating state inventory records, which does not follow their internal policy to ensure state inventory compliance. (page 22) CCB's continuous vulnerability management program includes several areas without oversight or operating procedures and limited documentation. (page 24) CCB utilizes the State's enterprise-managed security awareness training and simulated phishing platform as their primary cybersecurity training tool. We evaluated the security awareness training program of CCB and found there could be some improvements to CCB's procedures. (page 26)

Employment Security Division (ESD)

Summary: Information system controls at ESD need improvement to strengthen security and improve oversight of the operating IT environment. Weaknesses identified include: an overall risk assessment for ESD's operating IT environment remains undocumented, the asset inventory process lacks consistency and completeness, the continuous vulnerability management program lacks documentation and training, and the security awareness training program does not adhere to internal policies.

Key Findings: An overall security risk assessment for ESD's operating IT environment remains undocumented. (page 29) ESD depends on the Department of Employment, Training, and Rehabilitation's (DETR) IT team and an internal group to manage its computer inventory process. The agency has an internal inventory policy, but it has not been updated in over 16 years. (page 30) DETR's Information Security Officer oversees ESD's continuous vulnerability management program. During the audit, DETR was using the State's enterprise-managed vulnerability management software for vulnerability scanning. Out of 54 devices tested, 33 (61%) were scanned and each had at least one critical or high vulnerability. (page 31) ESD utilizes the State's enterprise-managed security awareness training and simulated phishing platform as their primary cybersecurity training tool. At the time of this audit, internal policies for follow-up on incomplete training were not consistently enforced. (page 33)

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

NORTHERN NEVADA
LEGISLATIVE BUILDING
401 S. Carson Street
Carson City, NV 89701
(775) 684-6800

SOUTHERN NEVADA
LEGISLATIVE OFFICES
7120 Amigo Street
Las Vegas, NV 89119
(702) 486-2800

THE STATE OF NEVADA
LEGISLATIVE COUNSEL BUREAU

Legislative Commission
Legislative Building
Carson City, Nevada

This report contains the findings, conclusions, and recommendations from our performance audit of the Division of Public and Behavioral Health, the Office of the Secretary of State, the Cannabis Compliance Board, and the Employment Security Division. 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 improve functions relating to the security of the information systems.

This report includes 27 recommendations to improve the security of the information systems for the 4 agencies audited. 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

May 30, 2025
Carson City, Nevada

Multi-Agency Information Security Table of Contents

Introduction

Executive Summary

Multiple state agencies can improve their information security controls in the following four areas: 1) risk assessments, 2) security awareness training, 3) continuous vulnerability management, and 4) asset inventory. The agencies selected for this audit included the Department of Health and Human Services, Division of Public and Behavioral Health (DPBH); the Office of the Secretary of State (SOS); the Cannabis Compliance Board (CCB); and the Department of Employment, Training and Rehabilitation, Employment Security Division (ESD).

It is the State Chief Information Officer's direction that all state agencies within the Executive Branch of the Nevada State Government comply with the direction of the State Information Security Program Policy. The National Institute of Standards and Technology (NIST) Special Publications 800 Series and the NIST Cybersecurity Framework (CSF) provide continuing guidance for the ongoing development and revision of the State Information Security Program Policy. In addition, Nevada Revised Statutes (NRS) 603A was amended in 2019 to identify the Center for Internet Security (CIS) Controls as a baseline security framework for the Executive Branch of the Nevada State Government.

State agencies have the responsibility to establish and implement a departmental security program, including policies, standards, and procedures. These are to be consistent with or exceed the requirements of the state security policy, and commensurate with the risk and magnitude of harm to state information resources. Information security controls are essential for maintaining the integrity, confidentiality, and availability of information. Neglecting any aspect of security controls can lead to potential security compromises.

To enhance cybersecurity resilience, numerous critical security controls play a vital role in safeguarding systems and data. We exercised professional judgment to select the following four key information security controls for testing.

Risk Assessment

For all agencies tested, the risk assessment process needs significant improvement. Risk assessments help to define and establish necessary controls and processes, commensurate with the level of risks, required to protect a state agency's information processing infrastructure and information. Without this assessment, agencies are unable to determine the risks, threats, and vulnerabilities to their information technology (IT) systems, applications, information, operational controls, and processes.

Asset Inventory

We determined most agencies tested need minor improvements to their asset inventory process. CIS Controls specify IT asset inventory and control of enterprise assets programs should be used to actively manage all IT assets and to accurately know the totality of assets that need to be monitored and protected. Without inventory management, agencies cannot ensure security monitoring, incident response, system backup, state inventory reconciliation, and recovery of their IT assets.

Vulnerability Management

Vulnerability management needs minor improvement at agencies tested. CIS Controls indicate vulnerability management programs should be used to continuously assess and track vulnerabilities on all assets in order to remediate and minimize the window of opportunity for attackers. Without vulnerability management, agencies will not have timely threat information about software updates, patches, security advisories, threat bulletins, etc. to identify vulnerabilities.

Security Awareness Training

We observed most agencies tested need minor improvements to their security awareness training programs. CIS Controls specify that security awareness programs are used to influence behavior among the workforce by helping individuals to be security-conscious and properly skilled, thereby reducing cybersecurity risks to an agency. Without user-concentrated security training, it becomes easier for an attacker to entice a user to click a link or open an email attachment to install malware and gain access to an agency.

While our testing is focused on these four aforementioned areas, we are not concluding on the overall adequacy of the agency's information security environment. Our conclusions and recommendations should only be applied to the specific areas identified as noted in the body of this report.

Scope and Objective

The scope of our audit included a review of systems, policies, and procedures in place during calendar years 2023 and 2024. Our audit objective was to:

- Determine if the selected agencies have adequate information security controls in place over information security risk assessments, security awareness training, vulnerability assessments, and inventory management to ensure the protection of information technology systems and the data those systems process, store, and transmit.

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 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.

Division of Public and Behavioral Health

Background

The mission of the Division of Public and Behavioral Health (DPBH) is to protect, promote, and improve the physical and behavioral health of the people of Nevada. DPBH is a division of the Department of Health and Human Services.

DPBH manages a diverse range of sensitive data associated with its many programs including behavioral health information, public health information, and clinical services information, among others. As of February 2025, DPBH had 1,543 full-time employees of which 37 are dedicated IT positions.

Summary

Information system controls at DPBH need improvement to strengthen security, efficiency, and oversight of their operating IT environment. Weaknesses identified include:

- The risk assessment process does not include complete annual assessments as required by state policy, nor has a full risk assessment of the entire operating IT environment been conducted.
- The inventory and control of enterprise assets did not include a physical inventory of assets as required by state standards.
- The continuous vulnerability management program lacks documented procedures and the ability to track known vulnerabilities.
- The security awareness training program lacks internal policies and procedures that would further aid management in requiring users to complete training before access to state information and systems occurs.

DPBH - Risk Assessment Process

Needs Significant Improvement

State Information Security Program Policy Not Followed

DPBH has not conducted and documented a security risk assessment or an annual security controls self assessment as required by state standards. DPBH contracted with a National Institute of Standards and Technology (NIST) auditor from the federal Department of Health and Human Services who helped DPBH conduct several internal risk assessments. However, the assessments analyzed individual systems, not the whole operating IT environment as a full risk assessment would. Further, the assessments took place on average a year and a half ago or more, and as such do not meet the annual requirements for self-assessments.

DPBH indicated it was trying to follow NIST guidelines for risk assessments. Management believed risk assessments only needed to be completed every 3 years, yet a full risk assessment of the entire operating IT environment has not occurred. Further, self-assessments are only being done when new applications are brought on, but the assessments solely look at those individual applications and systems, not the security posture of the agency as a whole. See Appendix A on page 34 for related criteria.

Without a documented security risk assessment, DPBH cannot ensure it will effectively identify or evaluate the risks, threats, and vulnerabilities to their IT systems, applications, information, and operational controls and processes. This could lead to data breaches, disruption of operations, reputational damage, or financial losses.

Recommendations

DPBH 1. Develop and implement a risk assessment program, conducting a thorough evaluation of DPBH's systems and related information security controls.

DPBH 2. Establish monitoring procedures to ensure the risk assessments are performed or updated consistent with the state security policy.

DPBH - Asset Inventory Process

Needs Significant Improvement

Controls Over Enterprise IT Assets Lack Procedures to Conduct and Document a Physical Inventory

DPBH does not conduct a physical inventory of IT assets. In addition, 5 of the 204 assets selected for testing were not located on the Active Directory tracking list maintained by the agency. Further, the Active Directory tracking list lacked pertinent identifying information for some assets such as asset tags and serial numbers that would aid the agency in accurately documenting and tracking assets. The Active Directory is a directory service developed by Microsoft for Windows domain networks. It is used primarily in enterprise environments to manage and organize users, computers, and other resources within a network.

The agency also does not have documented policies and procedures for conducting an inventory. DPBH IT staff indicated that utilizing agency tools such as the Active Directory, the patch management system, and the ticketing system gave enough insight into their inventory and therefore did not prioritize developing policies and procedures and dedicating resources to conduct a physical inventory. However, without a physical inventory, reconciliation with the state inventory system cannot occur. See Appendix A on page 34 for related criteria.

During the audit, DPBH upgraded their ticketing system to a new application that they explained would allow them to add scannable barcodes to each machine for inventory purposes. DPBH IT management indicated they were in the process of implementing this application and conducting a physical inventory, but it was not complete during the time of our audit.

Agencies are unable to protect assets they are not aware of. Without complete and accurate visibility, DPBH cannot ensure proper security monitoring, incident response, system backup, state inventory reconciliation, or recovery. This lack of awareness

may inhibit agencies from identifying additional assets on the network, making it difficult to isolate threats and safeguard operations against adversarial access.

Recommendation

DBPH 3. Develop policies and procedures for conducting and documenting an annual physical inventory of IT assets that includes pertinent identifying information, reconciliation process, and supervisor review.

DPBH - Vulnerability Management Process

Needs Minor Improvement

Continuous Vulnerability Management Program Lacks Tracking Processes

DPBH does not have a policy or process in place to track how long a security vulnerability has been active nor does it have the ability to identify what vulnerabilities are being worked on or remediated. DPBH currently utilizes the State's enterprise-managed vulnerability management software to scan its devices. However, we observed the agency lacked procedures to document and track vulnerabilities identified in the scans. Auditors randomly selected 10 devices with critical or high vulnerabilities and none of the 10 had tickets or other tracking documentation that would indicate which vulnerability it was, when it was identified, who it was assigned to, or how long it had been active.

IT management indicated the agency does not have internal policies or procedures that it follows for vulnerability management. Further, the agency does not have a documented resolution process that includes the ability to track active, known, in-progress, or fixed vulnerabilities. The current process to address vulnerabilities relies on constant communication from the team on what vulnerabilities are being addressed, as well as group policy which allows for some updates or patches to be done on multiple devices at the same time. While the agency is addressing some vulnerabilities, not documenting or tracking their resolution inhibits the agency's ability to thoroughly identify and address active vulnerabilities. See Appendix A on page 34 for related criteria.

Without a robust and ongoing vulnerability management program, agencies risk missing crucial updates on software patches, security advisories, and threat bulletins. This lack of timely information may prevent them from prioritizing weaknesses based on their impact, increasing the likelihood of exploitation. Agencies that neglect regular vulnerability assessments and fail to address

identified issues also face a higher likelihood of having their assets compromised.

Recommendations

DBPH 4. Develop a policy to define security vulnerability remediation efforts based on risk as determined by the agency.

DPBH 5. Develop procedures to ensure detected vulnerabilities requiring attention are documented and tracked throughout the resolution process.

DPBH - Security Awareness Training

Needs Minor Improvement

Security Awareness Training Program Lacks Documented Policies

DPBH utilizes the State's enterprise-managed security awareness training and simulated phishing platform as their primary cybersecurity training tool; however, the agency does not have any internal policies specific to security awareness training. We found that while all users were properly enrolled in training, 36 of 1,392 (3%) users tested had not taken their training within the required timeline. All 36 users were over the 90-day grace period. Additional testing on these 36 found 60% of 10 randomly selected users still had not taken training after receiving several reminder notifications. State standards indicate that training should be completed within 90 days of the hire date or training anniversary date. See Appendix A on page 34 for related criteria.

DPBH IT management indicated that there were conversations with agency management on ways to enforce security awareness training requirements such as user account restrictions. However, agency management did not implement account restrictions for users not taking their training because it might cause a loss of work hours. IT management also indicated there were other discussions on alternative ways to enforce security awareness training on users, but an agreement was not reached. Therefore, there were no consequences for users who do not take their training within the required state standards timeframe.

If employees are not completing their security awareness training, especially upon hire, it significantly raises the agency's cybersecurity risk profile. Users, both intentionally and unintentionally, can cause incidents due to the mishandling of sensitive data, sending an email with sensitive data to the wrong recipient, losing a portable end-user device, or using the same password used on public sites.

Recommendations

DPBH 6. Develop a policy for administering and managing the security awareness training program.

DPBH 7. Develop a procedure to ensure users complete security awareness training within the required timelines.

Office of the Secretary of State

Background

The Secretary of State is elected to a 4-year term and is responsible for maintaining the official records of the acts of the Nevada Legislature and the Executive Branch of State Government. The Office of the Secretary of State (SOS) is organized into eight divisions: Commercial Recordings, Document Preparation Services Program/Domestic Partnerships/Nevada Lockbox, Elections, Executive Administration, Nevada Business Portal, Notary, Operations, and Securities.

SOS manages a diverse range of sensitive data including: state and local election information, candidate contribution and expenditure information, and confidential addresses for victims of domestic violence. As of February 2025, SOS had 139 full-time employees, of which 26 were dedicated IT positions.

Summary

Information system controls at SOS need improvement to strengthen security and improve oversight of the operating IT environment. Weaknesses identified include:

- The risk assessment process does not follow state policy requiring the completion of annual assessments.
- The inventory and control of enterprise assets lack consistency and completeness.
- The continuous vulnerability management program lacks documentation and robust remediation processes.
- The security awareness training program does not ensure all employees are completing their initial and annual training.

SOS - Risk Assessment Process

Needs Significant Improvement

State Information Security Program Policy Not Followed

SOS has not completed a full documented risk assessment or prepared an annual self-assessment of information security controls. Internal IT evaluations related to certain systems and areas of the operating IT environment had occurred in May of 2023; however, the scope of those reviews was limited to only those areas tested and not inclusive of the overall operating IT environment.

Comprehensive, fully documented risk assessments have not been a priority. SOS has prioritized other assessments relating to specific areas of its operating IT environment such as the payment card environment. However, there are no controls in place to ensure a full risk assessment is completed biennially, as required by standards. See Appendix A on page 34 for related criteria.

Without a documented security risk assessment, SOS cannot ensure it will effectively identify or evaluate the risks, threats, and vulnerabilities to their IT systems, applications, information, and operational controls and processes. This could lead to data breaches, disruption of operations, reputational damage, or financial losses.

Recommendations

SOS 1. Develop and implement a risk assessment program that complies with state standards, conducting a thorough evaluation of SOS's systems and related information system controls.

SOS 2. Establish monitoring procedures to ensure the risk assessments are performed or updated consistent with state security policy.

SOS - Asset Inventory Process

Needs Minor Improvement

Controls Over Enterprise IT Assets Lack Documented Processes

SOS conducts semi-formal annual inventory procedures; however, there are no documented procedures for conducting the annual inventory and pertinent information is missing. SOS assets included in its inventory contain an asset tag or serial number for identification. However, the majority of the most recently acquired assets in 2023 do not have the serial number recorded in the 2023 inventory.

Although SOS was able to locate or identify the status of all 10 assets randomly selected for testing, there was a lack of documented procedures and training on conducting the annual inventory processes. Moreover, the inventory contained outdated or missing critical details about assets, such as serial numbers, configuration, and status. See Appendix A on page 34 for related criteria.

Agencies are unable to protect assets they are not aware of. Without asset visibility, SOS cannot ensure proper security monitoring, incident response, system backup, state inventory reconciliation, or recovery. This lack of awareness may inhibit agencies from identifying additional assets on the network, making it difficult to isolate threats and safeguard operations against adversarial access.

Recommendations

SOS 3. Create documented inventory procedures to reflect current practices, include a supervisor review process, and ensure compliance with state inventory standards.

SOS 4. Ensure that all assets are included in the annual inventory and that all inventory lists are regularly updated with complete and accurate identifying information.

SOS - Vulnerability Management Process

Needs Minor Improvement

Continuous Vulnerability Management Program Lacks Formal Policies and Procedures

SOS lacks documented procedures for maintaining its vulnerability management program and tracking of vulnerabilities found in the operating IT environment. While all SOS devices are scanned regularly by the State's enterprise-managed vulnerability management software, only devices found with the vulnerability status of known exploitable are addressed for remediation, leaving hundreds of devices with some vulnerabilities not being remediated. While the known exploitable vulnerabilities are properly prioritized, during the audit we found that 339 of 465 (70%) of the devices in the SOS's operating IT environment were reported to have some vulnerabilities present. Some of these devices have been vulnerable for years.

Our testing at the SOS's facilities in Las Vegas and Carson City found that 23 randomly selected devices were successfully included in the vulnerability scan set up in their IT environment. Of the devices being scanned, we randomly selected 10 devices reported to have some vulnerabilities and found none of those devices had helpdesk tickets for remediation or other tracking documentation. A risk-based decision was made by the Information Security Officer and the Chief Information Technology Manager to focus their vulnerability remediation efforts on the devices that posed the highest risk to the agency due to limited resources. See Appendix A on page 34 for related criteria.

Without a robust and ongoing vulnerability management program, agencies risk missing crucial updates on software patches, security advisories, and threat bulletins. This lack of information may prevent them from prioritizing all weaknesses based on their impact, increasing the likelihood of exploitation. Agencies that neglect regular vulnerability assessments and fail to address identified issues face a higher likelihood of having their assets compromised.

Recommendation

SOS 5. Develop and document vulnerability remediation and monitoring procedures to assess risk and prioritize actions, including an escalation process for delayed remediation.

SOS - Security Awareness Training

Needs Minor Improvement

Security Awareness Training Program Does Not Meet State Standards

SOS utilizes the State's enterprise-managed security awareness training and simulated phishing platform as its primary cybersecurity training tool. All 129 agency employees were properly enrolled in the security awareness training program and required to complete their annual or initial training within the first 90 days of employment as required by state policy. However, training was not always completed on time. See Appendix A on page 34 for related criteria.

Several factors contributed to untimely security awareness training completion. First, the training was not consistently made available within 90 days of an employee's start date. However, when made available, 78% of employees completed it within 90 days. Second, employees are made aware of their required training via a singular email notification, and no additional email reminders are utilized. Supervisors are tasked with ensuring completion, but this is not tracked and leads to employees not completing their training. The agency lacks agency-specific policies and procedures for carrying out this program, resulting in deficiencies primarily due to the absence of procedures for enrolling and tracking users for training completion.

If employees are not completing their security awareness training, especially upon hire, it significantly raises the agency's cybersecurity risk profile. Users, both intentionally and unintentionally, can cause incidents because of mishandling sensitive data, falling prey to phishing scams and malware, sending an email with sensitive data to the wrong recipient, losing a portable end-user device, using weak passwords, or using the same password used on public sites.

Recommendations

SOS 6. Develop documented policies and procedures for the administration and management of the security awareness training program.

SOS 7. Utilize the available built-in email reminder system to notify employees, their supervisors, and security awareness training program administrators when training is near or overdue to ensure compliance with state standards.

Cannabis Compliance Board

Background

The Cannabis Compliance Board (CCB) was established during the 2019 Legislative Session and was signed into law by the Governor. The CCB consists of five Govenor appointed board members. The CCB governs Nevada's cannabis industry through strict regulation of all areas of its licensing and operations, protecting the public health and safety of citizens and visitors while holding cannabis licensees to the highest ethical standards.

CCB manages a diverse range of sensitive data, including the medical cannabis and adult-use programs information. As of February 2025, CCB had 104 full-time employees, of which 6 are dedicated IT positions.

Summary

Information system controls at CCB need improvement as there is a lack of documented policies and procedures, including monitoring procedures to ensure key responsibilities are completed. Weaknesses identified include:

- A full information security risk assessment has not occurred, an annual self-assessment of security controls is not occurring as required by state policy.
- The inventory and control of enterprise IT assets process does not fully follow CCB policy and is not finalized.
- Continuous vulnerability management program lacks full implementation, documentation, and consistency.
- The security awareness training program lacks documentation and consistent procedures.

CCB - Risk Assessment Process

Needs Significant Improvement

State Information Security Program Policy Not Followed

CCB has been active for over 4 years and has not conducted and documented a full information security risk assessment. Further, an annual self-assessment of the CCB's security controls is not occurring. No assessments have taken place while it has existed.

Management indicated that focusing on other areas of CCB prevented them from putting the necessary effort into conducting a full risk assessment or annual assessment of controls. See Appendix A on page 34 for related criteria.

Without a documented security risk assessment, CCB cannot ensure it will effectively identify or evaluate the risks, threats, and vulnerabilities to their IT systems, applications, information, and operational controls and processes. This could lead to data breaches, disruption of operations, reputational damage, or financial losses.

Recommendations

CCB 1. Develop and implement a risk assessment program, conducting a thorough evaluation of CCB's systems and related information security controls.

CCB 2. Establish monitoring procedures to ensure the risk assessments are performed or updated consistent with state security policy.

CCB - Asset Inventory Process

Needs Minor Improvement

Controls Over Enterprise IT Assets Lack Documented Procedures

While CCB is conducting an annual inventory of assets, they are not updating state inventory records, which does not follow their internal policy to ensure state inventory compliance. Nevada's state inventory records show 65 assets listed as CCB equipment that were never in their physical custody according to management. The equipment in question has appropriation unit codes belonging to different agencies and although CCB has never had this equipment, the information was not updated in state records. According to CCB, state accounting records take 2 years to accurately report dropped assets; therefore, by not updating state records, accurate inventory records continue to be delayed.

Management is not adhering to its process for reconciling inventory with state records to maintain compliance with the state policy and laws. CCB's management explained they did not update state records because they first wanted to have a more consistent internal inventory process and determine exactly how they should track inventory before reconciliation with the state inventory system. See Appendix A on page 34 for related criteria.

Agencies are unable to protect assets they are not aware of. Without an accurate inventory both internally and in the state system, CCB cannot ensure proper security monitoring, incident response, system backup, state inventory reconciliation, or recovery. This lack of awareness may inhibit agencies from identifying additional assets on the network, making it difficult to isolate threats and safeguard operations against adversarial access.

Recommendation

CCB 3. Develop procedures that ensure internal inventory records are reconciled to state records and the state records are updated in accordance with the annual inventory requirements.

CCB - Vulnerability Management Process

Needs Minor Improvement

Continuous Vulnerability Management Program Lacks Full Implementation, Documentation, and Consistency

CCB's continuous vulnerability management program includes several areas without oversight or operating procedures and limited documentation. When this audit began, CCB had implemented the State's enterprise-managed vulnerability scanning software in their operating IT environment; however, we discovered scanning was not occurring at the newly located Carson City office and vulnerabilities were not being addressed. CCB's management worked to make scanning operational in Carson City, but more work is needed as addressing identified vulnerabilities is currently not a focus.

CCB's Information Security Officer indicated that attention was focused on other areas, leaving vulnerability management unaddressed when the audit began. In addition, the Carson City location was not being scanned because CCB changed locations and documentation was not updated to scan the new location, resulting in inconsistent scanning results. While CCB has addressed this, the overall vulnerability management process is still under development and not functioning properly. Furthermore, CCB has not prioritized addressing vulnerabilities. See Appendix A on page 34 for related criteria.

Without a robust and ongoing vulnerability management program, agencies risk missing crucial updates on software patches, security advisories, and threat bulletins. This lack of timely information prevents them from prioritizing weaknesses based on their impact, increasing the likelihood of exploitation. Agencies that neglect regular vulnerability assessments and fail to address identified issues face a higher likelihood of having their assets compromised.

Recommendations

CCB 4. Develop a policy to define security vulnerability remediation efforts based on risk as determined by the agency.

CCB 5. Develop and implement procedures to ensure all systems are scanned and that detected vulnerabilities are documented, tracked, and resolved.

CCB - Security Awareness Training

Needs Minor Improvement

Security Awareness Training Program Lacks Documentation and Consistent Procedures

CCB utilizes the State's enterprise-managed security awareness training and simulated phishing platform as their primary cybersecurity training tool. We evaluated the security awareness training program of CCB and found there could be some improvements to CCB's procedures. For 2 of 94 users tested, we observed they were not enrolled in security awareness training. However, one of the users had an account that was archived and even though the user took training, the application showed the user as not enrolled in the current training program. The other user was unaware they should complete training since they administer the training.

Further, there are no procedures to ensure all active employees are enrolled in security awareness training. We also observed the process for adding and removing users is performed manually. This presents an increased risk of error as every time a change needs to occur it must be completed by an individual without any procedures to guide the process. See Appendix A on page 34 for related criteria.

If employees are not completing their security awareness training, it significantly raises the agency's cybersecurity risk profile. Users, both intentionally and unintentionally, can cause incidents because of mishandling sensitive data, falling prey to phishing scams and malware, sending an email with sensitive data to the wrong recipient, losing a portable end-user device, using weak passwords, or using the same password used on public sites.

Recommendation

CCB 6. Develop policies and procedures for administering and managing the security awareness training program, ensuring all system users are identified and included.

Employment Security Division

Background

The Employment Security Division (ESD) has a vision of creating success for businesses and Nevadans. ESD exists to empower a vibrant labor market in Nevada by creating business and worker connections with high-quality, demand-driven services. ESD's primary functions include Unemployment Insurance, Workforce Development, and the Commission on Postsecondary Education. ESD is a division of the Nevada Department of Employment, Training, and Rehabilitation (DETR).

ESD manages a diverse range of sensitive data including unemployment insurance information and licensing information related to postsecondary education. As of February 2025, the agency had 442 full-time employees with no dedicated IT positions. ESD does not have its own Information Security Officer for the security of its operating IT environment. Therefore, IT and information security support is provided by DETR.

Summary

Information system controls at ESD need improvement to strengthen security and improve oversight of the operating IT environment. Weaknesses identified include:

- The risk assessment process does not follow state policy requiring annual risk assessments.
- Asset inventory controls do not follow internal policy.
- Continuous vulnerability management program lacks documentation and consistency.
- The security awareness training program does not adhere to internal policies.

ESD - Risk Assessment Process

Needs Significant Improvement

State Information Security Program Policy Not Followed

An overall security risk assessment for ESD's operating IT environment remains undocumented. While some assessments are conducted by the Internal Revenue Service and the Social Security Administration for their respective systems, other systems have not been fully assessed. Specifically, state security standards require an assessment be completed when significant changes occur to the agency, office, or IT environment. ESD informed us that no risk assessment was completed before its current modernization project started.

DETR's Information Security Officer indicated various aspects of ESD's operating IT environment were reviewed, but we found an adequate risk assessment program was not developed or implemented. In addition, there were no monitoring controls in place to ensure a risk assessment was completed routinely, as required by standards. See Appendix A on page 34 for related criteria.

Without a documented security risk assessment, ESD cannot effectively identify or evaluate the risks, threats, and vulnerabilities to their IT systems, applications, information, and operational controls and processes. This could lead to data breaches, disruption of operations, reputational damage, or financial losses.

Recommendations

ESD 1. Develop and implement a risk assessment program in compliance with state standards and conduct a thorough evaluation of ESD's systems and related information security controls.

ESD 2. Establish monitoring procedures to ensure the risk assessment is performed or updated consistent with state security policy.

ESD - Asset Inventory Process

Needs Minor Improvement

Asset Inventory Controls Do Not Follow Internal Policy

ESD depends on DETR's IT team and an internal group to manage its computer inventory process. The agency has an internal inventory policy, but it has not been updated in over 16 years. In addition, ESD's annual inventory spreadsheet lacked completion dates and other identification fields, but did contain the asset tag numbers required for inventory.

Of the 56 physical computers selected for testing, 17 (30%) were not found on the current inventory list. Furthermore, 1 of 10 computers randomly selected from the inventory list could not be located by the agency. Finally, ESD's management does not adhere to its internal process of reconciling internal inventory with the state inventory system. See Appendix A on page 34 for related criteria.

Agencies are unable to protect assets they are not aware of. Without asset visibility, ESD cannot ensure proper security monitoring, incident response, system backup, state inventory reconciliation, or recovery. This lack of asset reconciliation may inhibit agencies from identifying additional assets on the network, making it difficult to isolate threats and safeguard operations against adversarial access.

Recommendations

ESD 3. Update inventory procedures to comply with agency policy and establish a monitoring process to ensure proper implementation.

ESD 4. Develop an inventory reconciliation process to ensure the internal inventory and state system inventories match.

ESD - Vulnerability Management Process

Needs Minor Improvement

Continuous Vulnerability Management Program Lacks Documentation and Consistency

DETR's Information Security Officer oversees ESD's continuous vulnerability management program. During the audit, DETR was using the State's enterprise-managed vulnerability management software for vulnerability scanning. Out of 54 devices tested, 33 (61%) were scanned and each had at least one critical or high vulnerability. Ten of 33 were selected for further review. We found that 7 of 10 (70%) devices with vulnerabilities were not tracked on the internal monitoring sheet and lacked assigned resolution tickets. Two devices did have tickets but were closed despite the agency's vulnerability management software continuing to report the vulnerabilities. Only 1 of 10 devices tested had its vulnerabilities resolved.

Additionally, not all networks at the Las Vegas locations were scanned successfully, including some servers. However, this issue was being addressed during our audit. While the resolution process includes records of addressed vulnerabilities, it is inconsistently applied and some tickets are closed before the vulnerabilities are fully resolved. DETR's Information Security Officer did not ensure ESD's internal policies were being followed. See Appendix A on page 34 for related criteria.

Without a robust and ongoing vulnerability management program, agencies risk missing crucial updates on software patches, security advisories, and threat bulletins. This lack of timely information prevents them from prioritizing vulnerabilities based on their impact, leaving them vulnerable to exploitation. Agencies that neglect regular vulnerability assessments and fail to address identified issues face a higher likelihood of having their devices compromised.

Recommendations

ESD 5. Establish a procedure to ensure all devices and networks are being scanned and document any exceptions.

ESD 6. Establish procedures to ensure detected vulnerabilities are monitored, prioritized, and resolved.

ESD - Security Awareness Training

Needs Minor Improvement

Security Awareness Training Program Policies Were Not Consistently Enforced

ESD utilizes the State's enterprise-managed security awareness training and simulated phishing platform as their primary cybersecurity training tool. At the time of this audit, internal policies for follow-up on incomplete training were not consistently enforced. Of the 453 users enrolled in the training, 7 (2%) had overdue courses. Although these users received email reminders, follow-up efforts stopped after 4 weeks with no additional action taken. Further, three users were not assigned security awareness training and did not complete the training.

ESD's documented policy requires user accounts to be disabled by the Information Security Officer if the training was not completed; however, we found no evidence of this occurring. Additionally, the security awareness training platform was configured to stop sending email reminders after 4 weeks, allowing users continued network access without completing state-mandated training. Finally, the agency lacks a monitoring process to ensure that all users are added to the security awareness training group. See Appendix A on page 34 for related criteria.

If some employees are not completing their security awareness training, especially upon hire, it significantly raises the agency's cybersecurity risk profile. Users, both intentionally and unintentionally, can cause incidents because of mishandling sensitive data, sending an email with sensitive data to the wrong recipient, losing a portable end-user device, using weak passwords, or using the same password used on public sites.

Recommendation

ESD 7. Develop a monitoring procedure that ensures state security policies for the security awareness program are followed.

Appendix A
Relevant Audit Criteria

Select Nevada Revised Statutes

NRS 333.220 - Personal property of using agencies: Classification; identification; records; list of lost, excess, forfeited or donated property; transfers; inventories; regulations relating to condemnation and sale; determination of value; refurbishment.

4. The records of personal property of the State must be maintained at all times to show the officers entrusted with the custody thereof and transfers of that property between those officers. Each using agency shall conduct an annual physical count of all personal property charged to it and reconcile the results of the annual physical count with the records of inventory maintained by the Administrator. The Administrator shall maintain the current records of inventory for each state agency.

Select State of Nevada, State Information Security Program Policies

2.3 Roles and Responsibilities

2.3.2 State Agencies

State agencies have the responsibility to:

A: establish and implement a departmental security program, including policies, standards, and procedures, that is consistent with or exceeds the requirements of this policy, and commensurate with the risk magnitude of harm of state information resources should unauthorized access, use, disclosure, disruption, modification or destruction occur.

2.3.3 State Agency Information Security Officers

State Agency Information Security Officers (ISOs) have the responsibility to:

A: ensure the establishment, implementation, enhancement, monitoring, and enforcement of the federal, state, and agency information security policies and standards;

C: facilitate compliance with state and agency policies, standards, and procedures.

3.7 Risk Assessment and Risk Management

3.7.1 Risk Assessments

A: A full risk assessment must be conducted at each state agency to determine the risks, threats, and vulnerabilities to their IT systems, applications, information, and operational controls and processes. The full risk assessment must include;

1) **security administration assessment** of information security controls, policies, standards, procedures and processes, data classification, and information security plans;
2) **vulnerability assessments** of IT systems and applications, including networks, servers, wireless, websites, email systems, and data access controls, and
3) **physical security assessments** of agency offices for physical access and environmental controls.

D: The appropriate assessment must be conducted prior to the introduction of a new system application or when a major change occurs in the operating environment.

3.7.2 Self-Assessments

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

5.11 Security Testing and Vulnerability Assessment

All state systems and networks must have vulnerability scans and/or penetration tests to identify security threats prior to the initiation of a new system or network.

6.1 Inventory and Control of Hardware Assets

6.1.4 Maintain Detailed Hardware Asset Inventory

State agencies must maintain an accurate and up-to-date inventory of all hardware assets, including but not limited to, computer equipment, communications equipment, removable media, and other equipment, whether connected to the agency's network or not.

Select State Information Security Standards

S.2.05.01 Information Security Evaluations

6.0 Standard

6.1 All agencies shall conduct an initial security evaluation to determine the degree to which existing assets are protected against or exposed to unauthorized access or disclosure, modification, or loss.

6.5 All security evaluations shall be documented.

S.3.03.01 Information Security Officer Roles and Responsibilities

6.3 ISO Responsibility

C: Develop, implement, and maintain an information assets risk management and assessment program.

O: Ensure that valid asset inventory information is available, current, and auditable, including inventories of hardware, software, application systems, and system users.

S.3.07.01 Information Security Risk Analysis

6.0 Standard

6.1 Each agency shall perform or update a comprehensive risk analysis at least biennially or when significant changes occur to the agency, office, or IT environment. The analysis shall determine potential loss, identify areas of vulnerabilities, and evaluate existing controls, with the results documented in a Risk Analysis Report.

S.6.03.02 Vulnerability Management

6.0 Standard

6.1 Run automated vulnerability scanning tool.

B: Agencies must have a documented procedure in place for automatically scanning all devices on their network, both managed and unmanaged, on at least a weekly basis.

6.2 Perform authenticated vulnerability scanning.

A: Agencies must implement local scanning agents on each of their devices or configure remote scanners to perform authenticated vulnerability scans of every system on their network. All scans must be performed with the required credentials and elevated privileges to perform authenticated scans.

6.5 Utilize a risk-rating process

B: Agencies must prioritize the remediation of identified vulnerabilities based on the criticality assigned by their risk-rating methodology.

C: Agencies must have a documented process in place detailing their selected risk-rating and prioritization methodologies for vulnerability management.

S.6.17.01 Information Security Awareness and Training Program

6.0 Standard

6.3 The Informational Security Officer (ISO) shall coordinate efforts with the agency personnel or training section to ensure that all new and existing employees, consultants, and contractors attend an orientation program that introduces information security awareness and inform them of information security policies and procedures. This training must be completed within 90 days of each individual's hire date or awareness training anniversary date. All employees, consultants, and contractors who have access to information systems must acknowledge the security requirements of the system and their responsibility to maintain the security of the systems before access to the system is granted.

6.4 Acknowledgment of IT Security Awareness Training and/or Orientation occurs by signing a security awareness document indicating they understand their rights and responsibilities upon completion of the security awareness training and/or employee orientation. The ISO will determine the content of this document and how often this acknowledgment should be renewed. Security awareness training must be reinforced at least annually.

Appendix B
Audit Methodology

To gain an understanding of the selected agency's information technology (IT) security controls, we interviewed management, IT security personnel, and IT operations personnel. Through discussions and documentation review, we gained a broad understanding of how certain areas of IT security are managed at the selected agencies. In addition, we reviewed the State Information Security Program Policies, Standards, and Procedures; the National Institute of Standards and Technology (NIST) SP 800-53 Rev.5; the Center for Internet Security (CIS) Controls; and the Nevada Administrative Code (NAC). We also reviewed the selected agencies' policies, financial information, budgets, and other information describing their activities. Specifically, we documented and assessed internal controls over risk assessments, security awareness training, vulnerability management, and asset inventory.

To determine which agencies to include in this multi-agency audit, we performed a risk assessment. Using this information, we judgmentally selected four state agencies based on agency size, age, and organizational information security structure. Our audit included a review of the Division of Public and Behavioral Health (DPBH), the Office of the Secretary of State (SOS), the Cannabis Compliance Board (CCB), and the Employment Security Division's (ESD) 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 entities. The scope of our work on controls includes the following:

- Demonstrate commitment to integrity and ethical values; exercise oversight responsibility; establish structure, responsibility, and authority; and evaluate performance and enforce accountability (Control Environment);
- Define objectives and risk tolerances; identify, analyze, and respond to risks; assess fraud risk; and identify, analyze, and respond to changes (Risk Assessment);
- Implement control activities through policy (Control Activities);
- Use quality information; communicate internally; and communicate externally (Information and Communication);
- Perform monitoring activities; and evaluate issues and remediate deficiencies (Monitoring).

Deficiencies and related recommendations to strengthen the selected agencies' internal control systems are discussed in the body of this report. The design, implementation, and ongoing compliance with internal controls are the responsibility of agency management and agency Information Security Officers. For all populations obtained throughout the engagement, we observed extraction of the population from its source, noting that the parameters appeared sufficient, and the computer-generated information was reliable for our audit purposes.

To analyze the risk assessment process at each agency, we requested the most recent full information security risk assessment documentation. If a full risk assessment was available, we requested a list of new systems or major system changes to the operating IT environment for the last 12 months to assess if those system additions or changes were considered in the risk assessment. Finally, we requested the most recent self-assessment of current security controls to verify if it had been conducted at least annually for the last 2 years.

To test the security awareness training process at each agency, we obtained the agency's security awareness training program documentation and procedures, including a list of employees who had completed security awareness training for 2024. In addition,

we obtained a list of active employees from calendar year 2024 from the State Human Resources Data Warehouse system to compare to the security awareness training enrollment and completion list. We tested up to 10 users who did not complete security awareness training and 100% of the users who were not enrolled in security awareness training.

To test the continuous vulnerability management (CVM) process at each agency, we obtained their CVM program documentation and procedures. We requested a list of devices being scanned from the CVM system and randomly selected 5% of the computer population by visiting various sites and selecting physical computers to verify those systems were scanned and if the identified vulnerabilities had a resolution process initiated. For DPBH, 212 computers were selected from a population of 4,247. For SOS, 23 computers were selected from a population of 460. For CCB, 16 computers were selected from a population of 318. For ESD, 55 computers were selected from a population of 1,093. In addition, we observed the resolution process to verify how each agency handled the scan results.

To analyze the Inventory and Control of Enterprise Assets (ICEA) process at each agency, we obtained their authorized ICEA program documentation and procedures. In addition, we requested from the agency the most recent asset inventory list of devices that can store or process data. We then randomly selected 10 computers from the list and verified they could be located physically by the agencies. Finally, we randomly selected 5% of the computer population by visiting various sites and selecting physical computers to compare to the inventory list. We then determined if the computers selected from the population were missing from the inventory list by comparing the two lists. For DPBH, 212 computers were selected from a population of 4,247. For SOS, 23 computers were selected from a population of 460. For CCB, 16 computers were selected from a population of 318. For ESD, 54 computers were selected from a population of 1,093.

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. Within the scope and objective of this audit, we did not identify any vulnerabilities in information systems that posed a serious threat to the security of the agencies' information systems.

Our audit work was conducted from February 2024 to February 2025. 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, 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 selected agencies. We met with agency officials to discuss the results of the audit and requested a written response to the preliminary reports on the following dates: DPBH on May 15, 2025; SOS on May 13, 2025; CCB on May 12, 2025; and ESD on May 14, 2025. The responses are contained in Appendix C, which begins on page 42.

Contributors to this report included:

Joshua Terry, CISSP, CISA, PCIP
Deputy Legislative Auditor

Dalton Butler, CISA
Deputy Legislative Auditor

Christopher Gray, MPA
Deputy Legislative Auditor

Shirlee Eitel-Bingham, CISA
Audit Manager, Information Security

Todd Peterson, MPA
Chief Deputy Legislative Auditor

Appendix C

Response From Division of Public and Behavioral Health

Joe Lombardo
Governor

Richard Whitley, MS
Director

DEPARTMENT OF HEALTH AND HUMAN SERVICES

NEVADA DIVISION of PUBLIC and BEHAVIORAL HEALTH

Cody L. Phinney, MPH
Administrator

Ihsan Azzam, Ph.D., M.D.
Chief Medical Officer

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

Sent via email: dcrossman@lcb.State.nv.us

Dear Mr. Crossman,

Thank you so much for taking the time to meet with us on May 15, 2025, to complete the Audit Exit Conference. We value the information we received for your office and greatly appreciated the opportunity to work with you and your team to improve our internal policies and procedures.

As instructed, we have enclosed the Division of Public and Behavioral Health's (DPBH) response to the Legislative Auditor's Preliminary Audit Report on DPBH's Information Security. The Division has accepted all seven recommendations and has actively commenced remediating the findings stated in the report and codifying them in division policy and procedures.

Sincerely,

Cody L Phinney

Cody Phinney
DPBH Division Administrator

4150 Technology Way, Suite 300 • Carson City, NV 89706 • (775) 684-4200 • Fax (775) 687-7570 • dpbh.nv.gov

ALL IN GOOD HEALTH.

LCB Security Audit Findings & Remediation Plan Summary

1. Develop and implement a risk assessment program, conducting a thorough evaluation of DPBH's systems and related information security controls.

   Answer: DPBH agrees with this recommendation. The DPBH security team has created a procedure for Risk assessments based on the risk assessment completed in 2023 as well as the discovered needs of the division. The new risk assessment process will focus more on the Center for Internet Security (CIS) benchmarks determined to be primary security benchmarks for Nevada by the Office of the Chief Information Officer (OCIO) and Nevada Revised Statutes (NRS). Once these risk assessments are completed, they will be updated on an annual basis or whenever there are major system changes.

2. Establish monitoring procedures to ensure the risk assessments are performed or updated consistent with state security policy.

   Answer: DPBH agrees with this recommendation. While formal procedures were not previously documented, DPBH leverages tools to monitor for risks to our environment on a constant basis. Therefore, in conjunction with the risk assessment procedure, a policy has been drafted that ensures that DPBH risk assessments will meet or exceed the requirements of OCIO.

3. Develop policies and procedures for conducting and documenting an annual physical inventory of IT assets that includes pertinent identifying information, reconciliation process and supervisor review.

   Answer: DPBH agrees with this recommendation. In adherence to state policy set forth by the Nevada State Purchasing Division – Surplus Property unit, a physical inventory was in the process of being completed during the time of this audit. The 2025 completed physical inventory will be formally submitted to DPBH management by the end of June of 2025 for fiscal year 2024-25. The physical inventory policy and procedures have been developed to ensure annual completion using the same methodology and in accordance with state policy.

4. Develop a policy to define security vulnerability remediation efforts based on risk as determined by the agency.

   Answer: DPBH agrees with this recommendation. While it was not formally or clearly defined in our policy, DPBH follows industry best practices related to mitigating all security vulnerabilities and threats in our environment. From the recommendation of the LCB audit, formal policy and procedures have been developed based on the current practices of DPBH IT support staff.

5. Develop procedures to ensure detected vulnerabilities requiring attention are documented and tracked throughout the resolution process.

   Answer: DPBH agrees with this recommendation. A policy has been created to prioritize levels of vulnerabilities and set deadlines for remediation. Individual incidents or non-standard vulnerability findings will also be recorded and tracked in our help desk ticketing system.

6. Develop a policy for administering and managing the security awareness training policy.

   Answer: DPBH agrees with this recommendation. While a formal policy was not previously established, DPBH has been administering and managing an annual security awareness training program. We currently leverage a service through KnowBe4 which monitors, facilitates, and reports on security awareness training compliance for each employee in our organization. DPBH has followed the OCIO policy requiring annual security training based on the recommended training materials provided from OCIO. A policy has been created for the division that matches or exceeds the requirements of State policy.

4150 Technology Way, Suite 300 ● Carson City, NV 89706 ● (775) 684-4200 ● Fax (775) 687-7570 ● dpbh.nv.gov

7. Develop a procedure to ensure users complete security awareness training within the required timelines.

   Answer: DPBH agrees with this recommendation. To ensure compliance with the required timelines set forth by state policy, DPBH will continue to leverage our current tool for administering and monitoring security awareness training completion. Division policy will now emphasize DPBH adherence to the State policy of requiring all new employees and contractors to complete security awareness training within 30 days of hire, and annually thereafter. We will also ensure all employees, and their supervisors continue to be notified of their annual training requirement to maintain compliance.

4150 Technology Way, Suite 300 ● Carson City, NV 89706 ● (775) 684-4200 ● Fax (775) 687-7570 ● dpbh.nv.gov

ALL IN GOOD HEALTH.

Division of Public and Behavioral Health's Response to Audit Recommendations

Recommendations		Accepted	Rejected
DPBH 1.	Develop and implement a risk assessment program, conducting a thorough evaluation of DPBH's systems and related information security controls	X	
DPBH 2.	Establish monitoring procedures to ensure the risk assessments are performed or updated consistent with state security policy	X	
DPBH 3.	Develop policies and procedures for conducting and documenting an annual physical inventory of IT assets that includes pertinent identifying information, reconciliation process, and supervisor review	X	
DPBH 4.	Develop a policy to define security vulnerability remediation efforts based on risk as determined by the agency	X	
DPBH 5.	Develop procedures to ensure detected vulnerabilities requiring attention are documented and tracked throughout the resolution process	X	
DPBH 6.	Develop a policy for administering and managing the security awareness training program	X	
DPBH 7.	Develop a procedure to ensure users complete security awareness training within the required timelines	X	
TOTALS		7	

Response From Office of the Secretary of State

FRANCISCO V. AGUILAR
Secretary of State

RUBEN J. RODRIGUEZ
Deputy Secretary for Southern Nevada

DEANNA L. REYNOLDS
Deputy Secretary for Commercial Recordings

DEBBIE I. BOWMAN
Deputy Secretary for Operations

STATE OF NEVADA

OFFICE OF THE SECRETARY OF STATE

GABRIEL DI CHIARA
Chief Deputy Secretary of State

ERIN HOUSTON
Deputy Secretary for Securities

MARK A. WLASCHIN
Deputy Secretary for Elections

MEMORANDUM

To: Daniel Crossman – Legislative Auditor

From: Joshua Gruver – Chief IT Manager Secretary of State
CC: Gabriel Di Chiara – Chief Deputy Secretary of State

Date: May 19th, 2025

Subject: Response to Audit Findings

Dear Mr. Crossman,

This letter serves as the official response to the findings from the Legislative Audit which was performed by the Legislative Counsel Bureau's Audit Division on the Secretary of State's office. As an agency we appreciated the collaborative and professional interactions with all members of the audit team over the last year. We formally accept all the recommendations and have either completed them or are actively working toward their completion. Please see the next page for the status of all recommendations.

NEVADA STATE CAPITOL
101 N. Carson Street, Suite 3
Carson City, Nevada 89701-3714

PAUL LAXALT BUILDING
COMMERCIAL RECORDINGS
401 N. Carson Street
Carson City, Nevada 89701-4201

LAS VEGAS OFFICE
2250 Las Vegas Blvd North, Suite 400
North Las Vegas, Nevada 89030-5873

STATE OF NEVADA CAMPUS
1 State of Nevada Way, 3rd Floor
Las Vegas, Nevada 89119-4339

nvsos.gov

LCB Security Audit Findings and Remediation Status

1. **Develop and implement a risk assessment program that complies with state standards, conducting a thorough evaluation of SOS's systems and related information system controls.**
   Response: This process has been one that as an agency we've been aware of for years but unsuccessful in formally completing on a regular cadence with a consistent process. To finally bridge this gap we have purchased a Governance, Risk, and Compliance software package that will assist with automated risk assessments. The policy for utilization of the tool is being drafted during the ongoing implementation of the software package that is currently underway as of May 7th 2025. Estimated full compliance is at the end of July 2025.

2. **Establish monitoring procedures to ensure the risk assessments are performed or updated consistent with State Security Policy.**
   Response: Risk assessment tracking will be completed via the aforementioned tool from recommendation 1. Fully mature and established procedures are estimated to be implemented by the end of August 2025.

3. **Create documented inventory procedures to reflect current practices, include a supervisor review process, and ensure compliance with state inventory standards.**
   Response: The existing process and procedures are being reviewed in a collaborative effort between the information technology division and the accounting division that owns the procedure. The process is now being treated as an independent project with clear expectations and stakeholders. Full implementation and testing of the new procedures estimated to be completed during the next annual inventory which will occur November 2025.

4. **Ensure all assets are included in the annual inventory and that all inventory lists are regularly updated with complete and accurate identifying information.**
   Response: We have determined that we already possess the tools required to easily augment all required data fields to allow an accurate update of all technology assets with accurate information, allowing for easy confirmation of inventory status. This remediation was implemented in January 2025.

5. **Develop and document vulnerability remediation and monitoring procedures to assess risk and prioritize actions, including an escalation process for delayed remediation.**
   Response: The SOS information security team has drafted such procedures, and they have completed peer review and are now pending formal approval by leadership and then will be formally adopted. We have confirmed they adhere to and support all existing state security policies.

6. **Develop documented policies and procedures for the administration and management of the security awareness training program.**

   Response: The SOS information security team has drafted such procedures, and they have completed peer review and are now pending formal approval by leadership and then will be formally adopted. We have confirmed they adhere to and support all existing state security policies.

7. **Utilize the available built-in email reminder system to notify employees, their supervisors, and security awareness training program administrators when training is near or overdue to ensure compliance with state standards.**

   Response: The SOS information security team implemented this change, which covered all recommendations as written. This was successfully implemented in January of 2025.

Office of the Secretary of State's Response to Audit Recommendations

Recommendations		Accepted	Rejected
SOS 1.	Develop and implement a risk assessment program that complies with state standards, conducting a thorough evaluation of SOS's systems and related information system controls	X	
SOS 2.	Establish monitoring procedures to ensure the risk assessments are performed or updated consistent with state security policy	X	
SOS 3.	Create documented inventory procedures to reflect current practices, include a supervisor review process, and ensure compliance with state inventory standards	X	
SOS 4.	Ensure that all assets are included in the annual inventory and that all inventory lists are regularly updated with complete and accurate identifying information	X	
SOS 5.	Develop and document vulnerability remediation and monitoring procedures to assess risk and prioritize actions, including an escalation process for delayed remediation	X	
SOS 6.	Develop documented policies and procedures for the administration and management of the security awareness training program	X	
SOS 7.	Utilize the available built-in email reminder system to notify employees, their supervisors, and security awareness training program administrators when training is near or overdue to ensure compliance with state standards	X	
TOTALS		7	

Response From Cannabis Compliance Board

CANNABIS COMPLIANCE BOARD
STATE OF NEVADA

JOE LOMBARDO
Governor

ccb.nv.gov
CARSON CITY OFFICE
3850 Arrowhead Drive, Suite 100
Carson City, Nevada 89706
Main Line: (775) 687-6299

LAS VEGAS OFFICE
700 East Warm Springs Road, Suite 100
Las Vegas, Nevada 89119

JAMES HUMM
Executive Director

MICHAEL MILES
Deputy Director

ADRIANA GUZMÁN FRALICK
Chair

Daniel Crossman
Legislative Auditor
Nevada Legislative Counsel Bureau, Audit Division
401 S. Carson St., Carson City, NV 89701

Dear Mr. Crossman
The CCB has had the opportunity to review the Legislative Counsel Bureau's 2025 Performance Audit for the Cannabis Compliance Board ("CCB"). Based on the review of the findings, the CCB accepts the six recommendations related to the CCB.

The agency will develop and implement new policies and procedures and will revise existing procedures to address the audit findings and recommendations. The CCB's responses to each audit recommendation are enclosed.

On behalf of the CCB, I would like to thank you and your staff for your dedicated work and professionalism throughout this process. Further, the CCB has very much appreciated your guidance regarding improving operational efficiencies within the agency.

Please feel free to contact me if you have any questions or need clarification regarding this response.

Sincerely,

James Humm
Executive Director
Nevada's Cannabis Compliance Board

Recommendations

CCB 1. Develop and implement a risk assessment program, conducting a thorough evaluation of CCB's systems and related information security controls.

Response: The CCB accepts this recommendation.

Status: The CCB has completed a risk assessment for FY25 and is in the process of developing a risk assessment policy and procedure.

CCB 2. Establish monitoring procedures to ensure that risk assessments are performed or updated, consistent with state security policy.

Response: The CCB accepts this recommendation.

Status: Risk Assessment procedure development is in process.

CCB 3. Develop procedures that ensure internal inventory records are reconciled to state records, and the state records are updated in accordance with the annual inventory requirements.

Response: The CCB accepts this recommendation.

Status: The CCB is reviewing the agency's policy and procedures detailing the required process associated with inventory acquisition, maintenance, tracking, and disposition of fixed asset inventory.

CCB 4. Develop a policy to define security vulnerability remediation efforts based on risk as determined by the agency.

Response: The CCB accepts this recommendation.

Status: CCB vulnerability remediation policy is in development.

CCB 5. Develop and implement procedures to ensure all systems are scanned and that detected vulnerabilities are documented, tracked, and resolved.

Response: The CCB accepts this recommendation.

- **Status:** The CCB has already made progress on this recommendation to include vulnerability remediation procedures, fixes to the scanning plan and detection of vulnerabilities and tracking in a work tracking tool (JIRA) from identification through resolution.

CCB 6. Develop policies and procedures for administering and managing the security awareness training program, ensuring all system users are identified and included.

Response: The CCB accepts this recommendation.

Status: The CCB has already made progress on this recommendation to include implementation of a security awareness training acceptance policy and procedure, security awareness program policy and procedure and implemented the KnowB4 System to mitigate any missing users.

Cannabis Compliance Board's Response to Audit Recommendations

Recommendations		Accepted	Rejected
CCB 1.	Develop and implement a risk assessment program, conducting a thorough evaluation of CCB's systems and related information security controls.....	X	
CCB 2.	Establish monitoring procedures to ensure the risk assessments are performed or updated consistent with state security policy.....	X	
CCB 3.	Develop procedures that ensure internal inventory records are reconciled to state records, and the state records are updated in accordance with the annual inventory requirements	X	
CCB 4.	Develop a policy to define security vulnerability remediation efforts based on risk as determined by the agency.....	X	
CCB 5.	Develop and implement procedures to ensure all systems are scanned and that detected vulnerabilities are documented, tracked, and resolved	X	
CCB 6.	Develop policies and procedures for administering and managing the security awareness training program, ensuring all system users are identified and included	X	
TOTALS		6	

Response From Employment Security Division

EMPLOYMENT SECURITY DIVISION

Office of the Administrator

DETR
Nevada Department of Employment, Training and Rehabilitation

JOE LOMBARDO
Governor

CHRISTOPHER SEWELL
Director

KRISTINE NELSON
Administrator

TO: Daniel L. Crossman, CPA
Legislative Auditor
State of Nevada Legislative Counsel Bureau (LCB)

FROM: Kristine Nelson *Kristine Nelson*
Employment Security Division (ESD) Administrator
Department of Employment, Training and Rehabilitation (DETR)

DATE: May 23, 2025

SUBJECT: Multi-Agency Information Security Audit

This letter serves as the formal response to LCB's multi-agency information security audit, conducted in state fiscal year (SFY) 2025. As requested, attached is DETR ESD's response to audit recommendations form, and below are DETR ESD's responses to each of LCB's recommendations:

ESD 1. Develop and implement a risk assessment program in compliance with state standards and conduct a thorough evaluation of ESD's systems and related security controls.

a. DETR ESD acknowledges this recommendation.
b. DETR's Information Security Officer (ISO) team will update DETR's current **Control 140: Risk and Control Assessment** and **Control 125: Audit and Accountability** *policies* to ensure they are in line with current National Institute of Standards Technology (NIST) controls, state security policies, and in compliance with federal controls to access federal data (i.e., SSA, IRS).
c. DETR's ISO team will create a standard agency Risk and Control Assessment *procedure* in compliance with DETR's current **Control 140: Risk and Control Assessment** and **Control 125: Audit and Accountability** *policies* that will apply to all current systems and future system projects. This Risk Assessment *procedure* will be able to assess systems in their current state as well as any future systems being acquired.

500 East Third Street, Room 200 • Carson City, NV 89713 • (775) 684-3911• Fax (775) 684-3908
2800 E. St. Louis Avenue • Las Vegas, Nevada 89104 • (702) 486-7923 • Fax (702) 486-7924
detr.nv.gov

ESD 2. Establish monitoring procedures to ensure the risk assessment is performed or updated consistent with state security policy.

a. DETR ESD acknowledges this recommendation.
b. DETR's ISO team will review **Sec. 6.9 Continuous Monitoring** within its current **Control 140: Risk and Control Assessment** *policy* and **Sec. 12.0 Risk Management** within DETR's **Control 385: System Security Plan v. 3.5** and update, if necessary.
c. Said *policy* and *procedure* will be evaluated at least annually and updated as necessary.

ESD 3. Update inventory procedures to comply with agency policy and establish a monitoring process to ensure proper implementation.

a. DETR ESD acknowledges this recommendation.
b. In collaboration with DETR's Financial Management (FM) Purchasing Unit and DETR's ISO team, DETR ESD Management Administrative Support Services (MASS) will update DETR's current **Fixed Asset and Inventory**, **Control 150: Acquisition and Supply Chain** *policies*, as well as DETR's **Standard Operating Procedure (SOP) for Purchasing and Inventory** to ensure compliance with Nevada's current laws, regulations and policies to ensure proper control of DETR ESD inventory.
c. DETR ESD MASS will ensure that said policies and procedure updates include an inventory monitoring process.
d. DETR ESD MASS will disseminate said updated *policies* and *procedures* to DETR personnel and conduct annual inventory procedures training for DETR ESD personnel to monitor and measure inventory control compliance.

ESD 4. Develop an inventory reconciliation process to ensure the internal inventory and state system inventories match.

a. DETR ESD acknowledges this recommendation.
b. In conjunction with the actions stated above in **ESD 3**, DETR ESD MASS will ensure that an inventory reconciliation process is prescribed and communicated with DETR ESD staff in the *policies* and *procedure* updates stated above.
c. Said *policies* and *procedure* updates will include a new standard in line with current NIST controls, state security policies, and in compliance with federal controls (i.e., SSA, IRS).
d. DETR FM is responsible for the collection, reconciliation, and reporting of DETR's inventory to State Purchasing, which is conducted on an annual basis and certified each biennium.
e. Said *policies* and *procedures* will be evaluated at least annually and updated as necessary.

ESD 5. Establish a procedure to ensure all devices and networks are being scanned and document any exceptions.

a. DETR ESD acknowledges this recommendation.
b. DETR ISO maintains DETR's **Control 140: Risk and Control Assessment** *policy*, specifically **Sec. 6.7 Vulnerability Monitoring and Scanning;** and DETR's **Control 385: System Security Plan v. 3.5**, specifically **Sec. 7.6 Documentation** pertaining to vulnerability assessment reporting, which are established *policies* and *procedures* that the DETR ISO team follows and applies in its standard course of business.
c. Said *policies* and *procedures* will be evaluated at least annually and updated as necessary.

ESD 6. Establish procedures to ensure detected vulnerabilities are monitored, prioritized, and resolved.

a. DETR ESD acknowledges this recommendation.
b. As stated in **ESD 5,** above - DETR ISO maintains DETR's **Control 140: Risk and Control Assessment** *policy*, specifically **Sec. 6.7 Vulnerability Monitoring and Scanning;** and DETR's **Control 385: System Security Plan v. 3.5**, specifically **Sec. 7.6 Documentation** pertaining to vulnerability assessment reporting, which are established *policies* and *procedures* that the DETR ISO team follows and applies in its standard course of business.
c. Said *policies* and *procedures* will be evaluated at least annually and updated as necessary.

ESD 7. Develop a monitoring procedure that ensure state security policies for the security awareness program are followed.

a. DETR ESD acknowledges this recommendation.
b. DETR ISO maintains DETR's **Control 140: Risk and Control Assessment** *policy*, specifically **Sec. 6.7 Vulnerability Monitoring and Scanning;** and DETR's **Control 385: System Security Plan v. 3.5**, specifically **Sec. 3.0 Security Awareness** pertaining to *policies and procedures* pertaining to DETR's Security Awareness Program, which DETR's ISO team oversees and administers as the Department's standard course of business.
c. DETR's ISO team will review and update, as necessary, its current *policies* and *procedures* to ensure they reflect both state and federal data security requirements.
d. Said *policies* and *procedures* will be evaluated at least annually and updated as necessary.
e. DETR's ISO team currently uses the designated state-based Security Awareness Training Program (KnowBe4) to supply Security Awareness and Personal Identifiable Information training to all DETR personnel including contractors who access DETR's systems.

f. Notifications as a part of KnowBe4 settings are also sent to users and their supervisors for any training that is overdue.
g. Enforcement of training requirements is delegated to the appropriate supervisor of the DETR personnel supervisor of the user.

cc: Christopher Sewell, Director - DETR
Troy Jordan, Deputy Director – DETR
Joshua Marhevka, Deputy Director - DETR
Carl Stanfield, ITD Administrator, DETR

Employment Security Division's Response to Audit Recommendations

Recommendations			Accepted	Rejected
ESD	1.	Develop and implement a risk assessment program in compliance with state standards and conduct a thorough evaluation of ESD's systems and related information security controls	X	
ESD	2.	Establish monitoring procedures to ensure the risk assessment is performed or updated consistent with state security policy	X	
ESD	3.	Update inventory procedures to comply with agency policy and establish a monitoring process to ensure proper implementation	X	
ESD	4.	Develop an inventory reconciliation process to ensure the internal inventory and state system inventories match	X	
ESD	5.	Establish a procedure to ensure all devices and networks are being scanned and document any exceptions	X	
ESD	6.	Establish procedures to ensure detected vulnerabilities are monitored, prioritized, and resolved	X	
ESD	7.	Develop a monitoring procedure that ensures state security policies for the security awareness program are followed	X	
TOTALS			7	