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