LA24-14

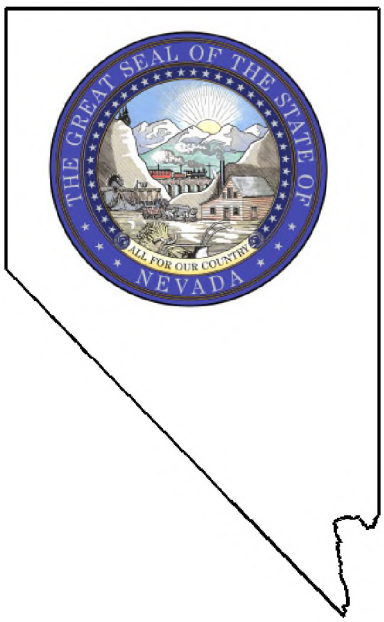
STATE OF NEVADA

Performance Audit

Silver State Health Insurance Exchange

Information Security

2023



Legislative Auditor
Carson City, Nevada

Audit Highlights

Highlights of performance audit report on the Silver State Health Insurance Exchange, Information Security issued on September 10, 2024.

Legislative Auditor report # LA24-14.

Background

The Silver State Health Insurance Exchange (Exchange) is the state agency that operates the online marketplace known as Nevada Health Link where eligible Nevada consumers can shop for, compare, and purchase quality and affordable health insurance plans. The Exchange facilitates and connects eligible Nevadans who are not insured by their employer, Medicaid, or Medicare to health insurance options. Individuals can purchase Affordable Care Act certified qualified health plans through the state-based exchange platform and, if eligible, can receive subsidy assistance to help offset their monthly premiums and out-of-pocket costs.

Established in 2011, the Exchange was created to function as a state-based health insurance exchange. However, from calendar year 2015 to the beginning of 2019, the Exchange utilized a federal platform called HealthCare.gov for the enrollment of Nevada residents. At the end of 2019, the Exchange transitioned to a state-based marketplace, NevadaHealthLink.com. The Exchange has contracted the enrollment, eligibility, and call center functions of the state-based exchange platform to a contractor.

Purpose of Audit

The purpose of the audit was to determine if the Exchange has adequate information security controls in place to protect the confidentiality, integrity, and availability of its information and information processing systems. Our audit focused on the systems and practices in place during fiscal years 2023 and 2024.

Audit Recommendations

This audit report contains 11 recommendations to improve information security controls of the Exchange's systems.

The Exchange accepted the 11 recommendations.

Recommendation Status

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

Information Security

Silver State Health Insurance Exchange

Summary

Improvements can be made to enhance information security controls meant to protect the confidentiality, integrity, and availability of the Exchange's systems. The Exchange's user access requests, authorizations, and monitoring practices were incomplete and undocumented. In addition, the Exchange does not verify that all users with access to the state-based exchange platform have completed a pre-access background check before granting system access. Furthermore, signed user access agreements have not been properly maintained or documented for all state-based exchange platform users. The Exchange's mandatory quarterly user access reviews have not been documented. In addition, security awareness training procedures and training policies have not been created or implemented. Finally, multiple users with state-based exchange platform access had not completed the assigned security awareness training, and the process to ensure completion was not effective.

The Exchange's key information security processes can be strengthened. In addition, the asset inventory process used at the Exchange needs to be further developed. Finally, the process for ensuring local administrator accounts are disabled needs to be implemented. Inadequate information security processes increase the risk of data loss, productivity loss, noncompliance, and reputational damage.

Our review of physical and environmental security controls concluded the Exchange can improve its key control process which includes physical and digital keycard management. Further, while the Exchange has a server room containing limited essential equipment and requires keycard access, the server room door provides minimal physical security. Physical security controls have a direct impact on the Exchange's ability to mitigate loss, disclosure, or inappropriate use of assets and protected data.

Key Findings

While we noted various opportunities for improvement, our work did not identify any critical security vulnerabilities at the Exchange within our testing areas. (page 4)

The Exchange's user access request practices lack consistency and documentation across the various user types accessing the state-based exchange platform. For 29 of the 30 users tested, the Exchange was unable to produce evidence of access request forms or other records of access approval. (page 4)

The Exchange's process for ensuring background checks are completed does not verify all users receive them. For the 30 users tested, the Exchange was unable to produce evidence it verified that a background check had been completed before granting or allowing access to the state-based exchange platform. (page 5)

The Exchange does not have a process in place to ensure all users accessing the state-based exchange platform, which contains Nevada citizens' personally identifiable information have read and signed the required acceptable use agreement. For the 30 state-based exchange platform users tested, the Exchange was unable to produce any documentation of a signed acceptable use agreement. (page 6)

The Exchange does not have any documentation to verify that quarterly user access reviews are being conducted. Exchange management explained to the auditors that a quarterly review is occurring; however, the review has never been documented and there is no formal process to perform or document quarterly reviews. (page 7)

Better oversight of the Exchange's security awareness training program for employees and contractors is needed. We identified 22 of 30 users tested did not complete their annual refresher security awareness training, or the Exchange was unable to produce evidence of its completion. (page 7)

The risk management process can be further developed to include an assessment of internal information technology (IT) systems. During discussions with management, it was confirmed that no risk assessment is completed for IT on the local Exchange network including servers and workstations. (page 9)

The Exchange's asset inventory practices are weak and need improvement as they relate to computer hardware used by the agency. After reviewing different reports of the Exchange's computer hardware assets, we observed significant discrepancies in physical inventory reconciliation. (page 10)

The Exchange does not adequately manage digital keycards and physical key access. While the Exchange utilizes the state's keycard access system, keycard accounts were not reviewed regularly to ensure the continued need for access to secure areas. (page 12)

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

Audit Division
Legislative Counsel Bureau

STATE OF NEVADA

LEGISLATIVE COUNSEL BUREAU

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

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

Legislative Commission
Legislative Building
Carson City, Nevada

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

This report includes 11 recommendations to improve information security controls of the Exchange's systems. We are available to discuss these recommendations or any other items in the report with any legislative committees, individual legislators, or other state officials.

Respectfully submitted,

Daniel L. Crossman, CPA
Legislative Auditor

July 9, 2024
Carson City, Nevada

Silver State Health Insurance Exchange
Information Security

Table of Contents

Introduction

Background

The Silver State Health Insurance Exchange (Exchange) is the state agency that operates the online marketplace known as Nevada Health Link where eligible Nevada consumers can shop for, compare, and purchase quality and affordable health insurance plans. The Exchange facilitates and connects eligible Nevadans who are not insured by their employer, Medicaid, or Medicare to health insurance options. Individuals can purchase American Care Act certified, qualified health plans through the state-based exchange platform and, if eligible, can receive subsidy assistance to help offset their monthly premiums and out-of-pocket costs.

Established in 2011, the Exchange was created to function as a state-based health insurance exchange. However, from calendar year 2015 to the beginning of 2019, the Exchange utilized a federal platform called HealthCare.gov for the enrollment of Nevada residents. At the end of 2019, the Exchange transitioned to a state-based marketplace, NevadaHealthLink.com. The Exchange has contracted the enrollment, eligibility, and call center functions of the state-based exchange platform to a contractor.

The vision of the Exchange is to provide access to affordable health insurance for all Nevadans. The mission is to increase the number of insured Nevadans by facilitating the purchase and sale of health insurance that provides quality health care through the creation of a transparent, simplified marketplace of qualified health plans.

The Exchange's Board of Directors consists of seven voting members and three ex officio nonvoting members. As of March 2023, the Exchange had 33 authorized positions with 31 positions filled, leaving a 6% vacancy rate. Exhibit 1 on the following page shows the Exchange's revenues and expenditures for fiscal year 2023.

Revenues and Expenditures **Exhibit 1**
Fiscal Year 2023

Revenues	Totals
Fees From Qualified Health Plan	$16,437,961
Transfer in FED ARPA	28,501
Total Revenues	**$16,466,462**
Expenditures	
Personnel	$ 2,173,072
Out of State Travel	7,526
In State Travel	13,218
Operating	322,851
Exchange Platform	6,220,823
Information Services	67,266
Training	7,774
Marketing and Outreach	3,201,237
Navigators	1,494,612
Transfer To Welfare Division	124,800
DHRM Cost Allocation	9,724
Purchase Assessment	17,293
Statewide Cost Allocation Plan	15,155
Total Expenditures	**$13,675,351**
Difference	$ 2,791,111
Plus: Beginning Cash	$ 8,755,512
Less: Reversion to General Fund	$ -
Balance Forward to 2024	**$11,546,623**

Source: State accounting system.

Scope and Objective

The scope of our audit covered the systems and practices in place during fiscal years 2023 and 2024. Our audit objective was to:

- Determine if the Exchange has adequate information security controls in place to protect the confidentiality, integrity, and availability of its information and information processing systems.

This audit is part of the ongoing program of the Legislative Auditor as authorized by the Legislative Commission and was made pursuant to the provisions of Nevada Revised Statutes 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.

Weaknesses Exist in User Management Controls

Improvements can be made to enhance information security controls meant to protect the confidentiality, integrity, and availability of the Exchange's systems. Specifically, the Exchange's user access requests, authorizations, and monitoring practices were incomplete and undocumented. In addition, the Exchange does not verify that all users with access to the state-based exchange platform have completed a pre-access background check before granting system access. Furthermore, signed user access agreements have not been properly maintained or documented for all state-based exchange platform users. The Exchange's mandatory quarterly user access reviews have not been documented. In addition, security awareness training procedures and training policies have not been created or implemented. Finally, multiple users with state-based exchange platform access had not completed the assigned security awareness training, and the process to ensure completion was not effective.

While we noted various opportunities for improvement, our work did not identify any critical security vulnerabilities at the Exchange within our testing areas.

User Access Requests Lack Consistency and Documentation

The Exchange's user access request practices lack consistency and documentation across the various user types accessing the state-based exchange platform. For 29 of the 30 users tested, the Exchange was unable to produce evidence of access request forms or other records of access approval. Without documentation of user account authorization, the Exchange cannot reasonably ensure the proper assignment of permissions or access. If user account reviews of the system are being completed, not having access request forms prohibits the

Exchange from accurately determining if users who have access are authorized.

The Exchange's management indicated implementing a system access request form would not strengthen access controls in their opinion, because internal personnel, certain contracted users (e.g., call center personnel), and enrollment assistants are assessed for system access needs to conduct essential job functions. However, documenting user access is essential for account review. According to state security standards, agencies that retain or have been given stewardship of data are responsible for determining who may have access to the data. In addition, criteria must be established in granting each user or class of users access to information and data.

Background Investigations Not Verified

The Exchange's process for ensuring background checks are completed does not verify all users receive them. For 30 users tested, the Exchange was unable to produce evidence it verified that a background check was completed before granting or allowing access to the state-based exchange platform. Our testing of user background checks included the Exchange, contracted, and other state-based exchange platform users.

For newly hired Exchange employees, there is no follow up to verify the completion of a background check prior to giving a new hire state-based exchange platform access. For contracted employees, the Exchange does not enforce its policy to have contractor background checks conducted by Nevada's Department of Public Safety (DPS). The Exchange provided background check completion dates for 10 contracted users and indicated the contractor assured them of their completion. However, these were not DPS background checks.

Without a complete and verified background check for users of the state-based exchange platform, the Exchange cannot reasonably ensure that the users accessing Nevada citizens' personally identifiable information (PII) do not have a criminal history, which increases the potential risk of unauthorized data access or use of the data. State security policy states that fingerprint-based background checks must be conducted on all persons hired,

promoted, or contracted for information technology (IT) services determined to be sensitive.

The Exchange's personnel security policy states that all State of Nevada employees and contractors are required by the Department of Administration, Division of Human Resource Management to complete a fingerprint-based background check conducted by the DPS, including Social Security, Federal Bureau of Investigation, and criminal background checks. Further, the Exchange's personnel security procedures state no personnel will be provided with unaccompanied physical access to the Exchange's office facilities, or logical access to the Nevada Health Link state-based exchange platform before the successful completion of this screening process.

Acceptable Use Agreements Not Signed

The Exchange does not have a process in place to ensure all users accessing the state-based exchange platform, which contains Nevada citizens' PII, have read and signed the required acceptable use agreement. For 30 exchange platform users tested, the Exchange was unable to produce any documentation of a signed acceptable use agreement. Exchange management has acknowledged that they have not kept proper records of signed agreements for internal personnel. Moreover, management stated the contractor is required to follow its own standards; therefore, the Exchange's policy and applicable state policies do not apply. However, this is contrary to the Exchange's policy. Finally, the Exchange indicated that for some users the acceptable use agreement is included in the annual certification process, but no documentation was provided for verification.

Failing to ensure acceptable use agreements are signed and in place by all system users before access is granted increases the risk of accidental data breaches. The Exchange's privacy impact assessment states all Exchange employees, contractors, and external stakeholders including: agents, brokers, navigators, and insurance carriers must read and sign the acceptable use agreement before being granted initial access to the state-based exchange platform and on at least an annual basis thereafter. The privacy impact assessment also requires that the Exchange

keep acceptable use agreements on hand for 5 years for its employees.

Routine User Access Reviews Not Documented or Verified

The Exchange does not have any documentation to verify that quarterly user access reviews are being conducted. Exchange management explained to the auditors that a quarterly review is occurring; however, it has never been documented and there is no formal process to perform or document quarterly reviews. Due to the lack of documentation, auditors cannot verify reviews are taking place.

Inadequate user access reviews regularly places the Exchange at higher risk for unauthorized system and data use. State security policy states that user accounts must be reviewed quarterly to ensure the continued need for access to a system. Additionally, accounts must be reviewed quarterly to ensure that transferred or reassigned users have been deleted. Any account that cannot be associated with an agency authorized user or state information system must be disabled.

Security Awareness Training Management Lacks Oversight

Better oversight of the Exchange's security awareness training program for employees and contractors is needed. We identified 22 of the 30 users tested did not complete their annual refresher security awareness training, or the Exchange was unable to produce evidence of its completion. Without a sufficient security awareness training program, there is an increased risk of loss or misuse of PII, loss of consumer and stakeholder confidence in the safety of data, unplanned costs associated with incident responses, loss of business critical data and systems, and increased rate of attacks in the future.

According to state security standards, all new and existing employees, consultants, and contractors must attend an orientation program that introduces information security awareness and informs them of information security policies and procedures. Standards also require security awareness training be reinforced annually. Despite these requirements, the Exchange has not created any validation procedures for contractors to ensure training is completed. Furthermore, the Exchange's IT staff indicated a training platform used by

employees is new and they are still working on updating the training content.

Recommendations

1. Develop and document a request, approval, and monitoring process for all types of users with state-based exchange platform access.
2. Develop a process to monitor the status of background checks for all required users to ensure they are being completed before granting system access.
3. Develop a background check verification process to ensure contractors are complying with policy requirements to have fingerprint-based background checks conducted by Nevada's Department of Public Safety.
4. Develop a process to ensure acceptable use agreements are completed and documented for all personnel accessing the state-based exchange platform.
5. Develop a formal process to perform and document quarterly user access reviews of all users accessing the state-based exchange platform.
6. Establish procedures to ensure all employees, vendors, and contractors receive initial and annual security awareness training and maintain an up-to-date list of completed training.

Key Information Security Processes Can Be Strengthened

The Exchange's key information security processes can be strengthened. Specifically, the Exchange lacks an internal risk assessment process and documentation. In addition, the asset inventory process used at the Exchange needs to be further developed. Finally, the process for ensuring local administrator accounts are disabled needs to be implemented. Inadequate information security processes increase the risk of data loss, productivity loss, noncompliance, and reputational damage.

Internal Risk Assessment Not Conducted

The Exchange's risk management process can be further developed to include an assessment of internal IT systems. During discussions with management, it was confirmed that no risk assessment is completed for IT on the local Exchange network including servers and workstations. Although an annual risk assessment is conducted by a contractor for the state-based exchange platform, the Exchange has not prioritized the assessment of risks on internal systems.

State security policy states agencies must conduct a self-assessment of their information security controls at least annually and revise their controls according to identified inadequacies or new risks. Without conducting a risk assessment there could be vulnerabilities to the local system that have not been identified. Vulnerabilities give cybersecurity adversaries the potential to gain access to the system through various kinds of attacks. Depending on the type of access gained, an adversary could gain unauthorized access to the state-based exchange platform which does contain sensitive PII of Nevada citizens.

Asset Inventory Process Needs Improvement

The Exchange's asset inventory practices are weak and need improvement as they relate to computer hardware used by the agency. After reviewing different reports of the Exchange's computer hardware assets, we observed significant discrepancies in physical inventory reconciliation. Specifically, we determined that 39 computers listed in state inventory records were not on the Exchange's physical inventory list, and two computers on the physical inventory list were not in the state inventory list. In addition, 5 of 15 computers judgmentally selected for testing, based on location in the office, were not present on the physical inventory list. Interviews with agency personnel demonstrated uncertainty regarding IT inventory and who is responsible at the Exchange for conducting the inventory. The Exchange did not have any documentation verifying when the last inventory took place.

According to state security policy, agencies must maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. Not maintaining an accurate asset inventory list increases the risk of theft or loss of agency assets as well as security breaches and data loss should the agency experience an incident and not be aware of what assets were effected.

Local Administrator Accounts Not Always Disabled

The Exchange does not always disable local administrator accounts. Local administrator accounts are used when setting up new computers. For 1 of the 10 workstations tested, the local administrator account was not disabled.

Although disabling this account is a best practice, the Exchange does not have onboarding or monitoring procedures to ensure local administrator accounts are disabled after setup. According to Microsoft's security considerations:

> Because the Administrator account is known to exist on many versions of the Windows operating system, it's a best practice to disable the Administrator account, when possible, to make it more difficult for malicious users to gain access to the server or client computer.

Local administrator access could provide attackers with more extensive or unbound access.

Recommendations

7. Create procedures to include local networked devices, systems, and servers in the annual risk assessment process.
8. Develop asset inventory procedures that account for all active and inactive information technology hardware and ensure the inventory is regularly updated.
9. Update onboarding procedures to ensure the local administrator account is disabled on workstations when the setup is complete and implement a monitoring process to ensure the procedure is followed.

Physical Security Controls Can Be Improved

Generally, physical access controls appeared sufficient; however, our review of physical security controls found the Exchange can improve its key control process, which includes digital keycard and physical key management. Further, while the Exchange has a server room containing limited essential equipment and requires keycard access, the server room door provides minimal physical security. Physical security controls have a direct impact on the Exchange's ability to mitigate loss, disclosure, or inappropriate use of assets and protected data.

Key Control Process Needs Attention

The Exchange does not adequately manage digital keycards and physical key access. While the Exchange utilizes the state's keycard access system, keycard accounts were not reviewed regularly to ensure the continued need for access to secure areas. After reviewing a list of active users from the digital keycard system, we found two users had incorrect last names in the system. Without conducting regular, documented inventories of digital keycards and key distribution, the Exchange cannot ensure users are authorized to access secure areas.

Additionally, while the Exchange does maintain manual forms for the distribution of physical keys, we found there was no record in the system of how many keys were originally distributed, turned in, or assigned a key number for tracking purposes. Further, 2 of 28 keys were lost or stolen as indicated in documentation, but documentation is inconsistent as some forms used were not filled out completely. Without a proper record of the number of physical keys originally distributed and turned in, there cannot be a viable record of the number of keys that exist; therefore, access to agency assets and sensitive information could be compromised.

State security policy states agencies must implement appropriate controls to limit access to rooms, work areas, and facilities that contain the agency's information systems, networks, and data to authorized personnel only. The Exchange does not have written policies and procedures regarding the management, distribution, collection, or review of keycard accounts and physical key inventory.

Server Room Security Should Be Enhanced

The Exchange's server room access controls can be enhanced. While the Exchange has a server room containing limited essential equipment and requires keycard access to enter the building and room, the server room door provides minimal physical security. The server room door is a regular wood-slated door that could easily be broken through. After inspecting the door, we concluded that the door was not sufficiently secure. The following picture shows the current server room door.

The Carson City Exchange's server room door.

Source: Picture taken by auditor.

As shown in the picture, the server room door's slats and exterior hinges would offer little resistance to a forced entry. This could potentially give unauthorized individuals access to the server room, functions, and sensitive information.

The Exchange has relied on other controls such as door access management to provide security and has not prioritized replacing the server room door with a door of solid core structure. State security policy states appropriate controls must be implemented to ensure that rooms, work areas and spaces, and facilities that contain IT resources that process, transmit, or store sensitive, or privacy information are protected from unauthorized access.

Recommendations

10. Develop a key inventory policy and keycard account review process for controlling access to secure areas.
11. Enhance the physical security of the server room.

Appendix A
Audit Methodology

To gain an understanding of the Silver State Health Insurance Exchange (Exchange), we interviewed staff, reviewed state information security standards, policies, laws, and administrative codes, and reviewed policies and procedures significant to the Exchange's operations. We also reviewed prior audit reports, financial information, budgets, and other information describing the Exchange's functions.

Through discussions with management and a review of associated documents and contracts, we gained an understanding of the state-based exchange platform and the relationship between the Exchange, agents, brokers, facilitators, other users, and contractors of the state-based exchange platform. Furthermore, we documented and assessed internal controls over user management, information security processes, and physical security controls.

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

- Exercise oversight responsibility, establish structure, responsibility, and authority, and demonstrate commitment to competence (Control Environment);
- Define objectives and risk tolerances (Risk Assessment);

- Design control activities, design information system control activities, and implement control activities through policy (Control Activities);

- Communicate internally (Information and Communication); and

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

Deficiencies and related recommendations to strengthen the Exchange's 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.

To evaluate whether current oversight of user management controls were sufficient, we requested a user list from the state-based exchange platform to include all users. We assessed the reliability of this list by verifying there were no duplicate email addresses. We randomly selected 30 of 2,449 users from the list: 10 Exchange users, 10 contracted users, and 10 other users to examine user management documentation. We requested documentation of access request forms, background investigation verification, signed acceptable use agreements, and security awareness training records for each of the 30 users. To conclude if the Exchange had proper oversight of user management including whether a routine review of accounts was being conducted, we compared our findings to the Exchange's policies and state security standards and policies.

To verify the Exchange is conducting risk assessments of the information technology environment, we requested the latest risk assessment completed to verify it complied with state security standards and Exchange's policies.

Furthering our security processes testing, we evaluated the asset inventory of computers at the Exchange. We requested an active directory list of all workstation equipment and we extracted an inventory list from the state accounting system. We requested all

documentation of an internal inventory completed physically by Exchange personnel and compared them against inventory listings. Next, we judgmentally selected 15 of about 55 computers based on location from the Exchange's Carson City office and verified the computers were listed in the same 3 lists. Finally, we judgmentally selected 10 computers from the Carson City location to verify if the local administrator accounts on those computers were disabled.

To evaluate whether current oversight of physical security controls was sufficient, we tested physical key and digital keycard controls related to building access. We requested a list of users with physical and electronic access to the agency. We compared the list extracted from the Department of Administration, Division of Human Resources Management, data warehouse system to validate the reliability of the list from the agency. Using 100% of the 29 users, we confirmed current access rights were authorized by comparing to keycard documentation.

Finally, we tested the server room door to make sure proper security controls were in place. We visually observed the door to determine if it could withstand a forced entry attempt as well as checked for entry controls such as keycard access to prevent unauthorized access.

We used nonstatistical audit sampling for our audit work, which was the most appropriate and cost-effective method 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.

Our audit work was conducted from March 2023 to January 2024. 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 Executive Director of the Silver State Health Insurance Exchange. On June 24, 2024, we met with agency officials to discuss the results of the audit and requested a written response to the preliminary report. That response is contained in Appendix B, which begins on page 19.

Contributors to this report included:

Christopher Gray, MPA
Deputy Legislative Auditor

Dalton Butler, BS
Deputy Legislative Auditor

Shirlee Eitel-Bingham, CISA
Audit Manager, Information Security

Todd Peterson, MPA
Chief Deputy Legislative Auditor

Appendix B

Response From the Silver State Health Insurance Exchange

Joe Lombardo
Governor

Valerie Clark
Vice - Chairwoman

Russell Cook
Executive Director

Silver State Health Insurance Exchange

2310 South Carson Street, Suite 2 Carson City, NV 89701 T: 775-687-9939 F: 775-687-9932

www.nevadahealthlink.com/sshix

Daniel L. Crossman, CPA
Legislative Auditor
Legislative Building
401 S. Carson Street
Carson City, NV 89701-4298

Dear Mr. Crossman:

This letter serves as a response to the recent Legislative Auditors Performance Audit conducted on The Silver State Health Insurance Exchange.

We appreciate the opportunity to engage over the past year, reviewing and discussing the audit findings. Leveraging these discussions and the detailed information provided, our team has actively started to revise and enhance our policies and procedures. This effort aims to address the audit findings effectively and ensure the Silver State Health Insurance Exchange operates with the highest efficiency and effectiveness.

The Silver State Health Insurance Exchange have accepted all the recommendations outlined in the audit and have included a summary of the items that have been implemented, those currently in progress, and those that are being finalized.

1. Develop and document a request, approval, and monitoring process for all types of users with state-based exchange platform access.

   Silver State Health Insurance Exchange is currently in the process of developing and documenting a comprehensive policy that includes a request, approval, and monitoring process for all user types accessing the state-based exchange platform. This policy aims to ensure secure and efficient management of user access, aligning with best practices and compliance requirements.

2. Develop a process to monitor the status of background checks for all required users to ensure they are being completed before granting system access.

   Silver State Health Insurance Exchange is developing a process to monitor the status of background checks for all required users to ensure they are completed before granting system access. This process will include regular tracking and verification steps to maintain security and compliance standards.

3. Develop a background check verification process to ensure contractors are complying with policy requirements to have fingerprint-based background checks conducted by the Nevada's Department of Public Safety.

The State Health Insurance Exchange have been working with the vendor to find a solution that will work for our out-of-state contractors to ensure compliance with the policy requirements for fingerprint-based background checks conducted by Nevada's Department of Public Safety. This will help us verify that all contractors meet the necessary security standards.

4. Develop a process to ensure acceptable use agreements are completed and documented for all personnel accessing the state-based exchange platform.

   The State Health Insurance Exchange is developing a process to ensure that acceptable use agreements are completed and documented for all personnel accessing the state-based exchange platform. This process will ensure that all users understand and acknowledge the terms of use, thereby maintaining compliance and promoting responsible usage of the platform.

5. Develop a formal process to perform and document quarterly user access reviews of all users accessing the state-based exchange platform.

   The State Health Insurance Exchange is in the process of developing a formal procedure to conduct and document quarterly user access reviews for all individuals accessing the state-based exchange platform. This initiative will ensure that access permissions are regularly reviewed and updated, enhancing security and compliance.

6. Establish procedures to ensure all employees, vendors, and contractors receive initial and annual security awareness training and maintain an up-to-date list of completed training.

   The State Health Insurance Exchange is currently conducting annual security awareness training through KnowBe4 for all employees. We are also working closely with the appropriate staff from vendor companies to ensure that their personnel receive similar training. This ensures that everyone is up-to-date with the latest security practices. Additionally, we are maintaining an updated list of all completed training sessions to ensure compliance and track progress.

7. Create procedures to include local networked devices, systems, and servers in the annual risk assessment process.

   During the month of July, the State Health Insurance Exchange initiated our first risk assessment that includes local networked devices, systems, and servers. Moving forward, we plan to conduct this comprehensive risk assessment annually every July to ensure all components are thoroughly evaluated and any potential risks are promptly addressed.

8. Develop asset inventory procedures that account for all active and inactive information technology hardware and ensure the inventory is regularly updated.

State Health Insurance Exchange have made significant progress in reducing the excess equipment across our offices. To ensure our asset inventory remains accurate and up-to-date, we are planning to conduct bi-annual reviews in December and June. These reviews will account for all active and inactive information technology hardware, helping us maintain a streamlined and efficient inventory management process.

9. Update onboarding procedures to ensure the local administrator account is disabled on workstations when the setup is complete and implement a monitoring process to ensure the procedure is followed.

   State Health Insurance Exchange are in the process of updating our onboarding procedures to ensure that the local administrator account is disabled on workstations once setup is complete. As part of this initiative, we are implementing Microsoft Local Administrator Password Solution (LAPS) to enhance security. This will include a monitoring process to ensure the procedure is consistently followed and effectively maintained.

10. Develop a key inventory policy and keycard account review process for controlling access to secure areas.

    State Health Insurance Exchange are actively developing two draft policies aimed at enhancing security in our secure areas. These policies include a comprehensive key inventory policy and a keycard account review process. The goal is to ensure stringent control and monitoring of access to secure areas, thereby improving our overall security posture.

11. Enhance the physical security of the server room.

    State Health Insurance Exchange is currently working on finding a solution that ensures the server room hardware is maintained at an optimal temperature while simultaneously providing the necessary physical security.

Sincerely,

Max Borgman
Information System Manager
Silver State Health Insurance Exchange

Silver State Health Insurance Exchange's Response to Audit Recommendations

	Recommendations	Accepted	Rejected
1.	Develop and document a request, approval, and monitoring process for all types of users with state-based exchange platform access	X	
2.	Develop a process to monitor the status of background checks for all required users to ensure they are being completed before granting system access	X	
3.	Develop a background check verification process to ensure contractors are complying with policy requirements to have fingerprint-based background checks conducted by Nevada's Department of Public Safety	X	
4.	Develop a process to ensure acceptable use agreements are completed and documented for all personnel accessing the state-based exchange platform	X	
5.	Develop a formal process to perform and document quarterly user access reviews of all users accessing the state-based exchange platform	X	
6.	Establish procedures to ensure all employees, vendors, and contractors receive initial and annual security awareness training and maintain an up-to-date list of completed training	X	
7.	Create procedures to include local networked devices, systems, and servers in the annual risk assessment process	X	
8.	Develop asset inventory procedures that account for all active and inactive information technology hardware and ensure the inventory is regularly updated	X	
9.	Update onboarding procedures to ensure the local administrator account is disabled on workstations when the setup is complete and implement a monitoring process to ensure the procedure is followed	X	
10.	Develop a key inventory policy and keycard account review process for controlling access to secure areas	X	
11.	Enhance the physical security of the server room	X	
	TOTALS	11	