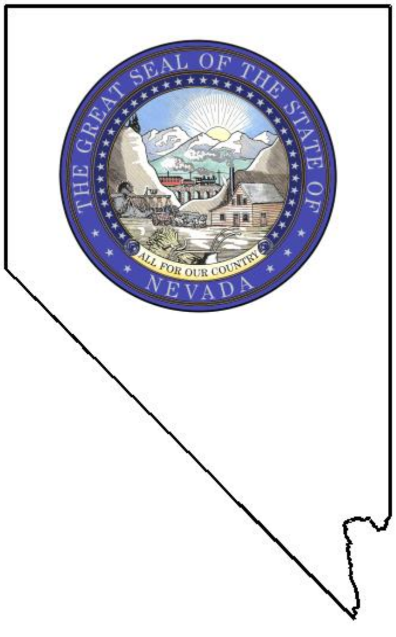
LA20-13

STATE OF NEVADA

Performance Audit

Public Employees' Benefits Program
Information Security

2020



Legislative Auditor
Carson City, Nevada

Audit Highlights

Highlights of performance audit report on the Public Employees' Benefits Program, Information Security issued on February 18, 2020.

Legislative Auditor report # LA20-13.

Background

The Public Employees' Benefits Program (PEBP) is a state agency that is legislatively mandated to provide group health, life, and accident insurance for state and other eligible public employees.

PEBP currently administers various benefits and is responsible for designing and managing a quality health care program for approximately 43,000 primary participants and 27,000 covered dependents, totaling over 70,000 individuals. PEBP's mission is to provide employees, retirees, and their families with access to high quality benefits at affordable prices.

A 10-member Board oversees PEBP's operations. Nine Board members are appointed by the Governor, and the 10th member is the Director of the Department of Administration or his designee approved by the Governor. The Board appoints an Executive Officer to direct the day-to-day operations.

Funding for PEBP operations and insurance plans comes primarily from participant and employer contributions. PEBP submits its funding and operational requirements to the Legislature as part of the biennial budget. Upon approval, each state agency is assessed an amount to contribute toward both the active-employee and retiree health plans. For fiscal year 2019, PEBP had revenues of more than $376 million.

Purpose of Audit

The purpose of the audit was to determine if PEBP has adequate information security controls in place to protect the confidentiality, integrity, and availability of its information and information systems. Our audit focused on the systems and practices in place during calendar year 2019 and included a review of security awareness training rosters from prior years.

Audit Recommendations

This audit report contains 14 recommendations to improve the security of PEBP's information systems.

PEBP accepted the 14 recommendations.

Recommendation Status

PEBP's 60-day plan for corrective action is due on May 12, 2020. In addition, the 6-month report on the status of audit recommendations is due on November 12, 2020.

Information Security

Public Employees' Benefits Program

Summary

The Public Employees' Benefits Program (PEBP) needs to strengthen its information system controls to ensure adequate protection of information systems and information processed therein. By taking action to address these control weaknesses, PEBP can better protect its physical resources, minimize security vulnerabilities, and ensure continuation of critical services.

Control weaknesses included: 1) inadequate security over computers and network devices, such as computers missing operating system and anti-virus updates; 2) not adequately managing users, including lack of account review and non-compliance with background check and security awareness training requirements; and 3) incomplete security related plans, such as lack of a current IT contingency plan and documentation of data recovery process.

Key Findings

PEBP is not monitoring the status of operating system updates on its computers and laptops. The application which PEBP utilizes to automate operating system updates did not successfully deploy updates to 13 of the 20 computers and laptops we tested. This problem went undetected as staff were not routinely verifying whether updates were installed successfully. Staff acknowledged additional training in the administration of the systems management application is needed to gain more familiarity with the system and its capabilities. (page 4)

PEBP is not ensuring its computers and laptops are current with anti-virus software. The application which automates anti-virus deployment was not successfully deploying virus definition updates to 24 of the 55 computers we tested. This problem went largely undetected as staff were not routinely verifying updates were installed successfully and were not familiar with the anti-virus management application. (page 5)

Weaknesses exist in managing PEBP's network accounts. Of PEBP's 110 network accounts, we identified 64 active user and service accounts that should be reviewed to determine their need. PEBP was disabling user accounts upon employee departure; however, it did not perform routine account maintenance to remove obsolete accounts. (page 8)

PEBP is not routinely reviewing user access privileges in five of its critical applications and user access is not removed in a timely manner. These applications contain personal identifying information. During our analysis of the critical applications, we determined that although PEBP had established a procedure for revoking user access upon employee termination, it was not being followed. (page 9)

Background checks were not completed for PEBP's IT contractors. During our system account review, we identified three IT contractor accounts. We determined none of these IT contractors had background checks conducted as part of their hiring process, although PEBP conducted routine background checks on employees. These IT contractors had access to important information systems containing sensitive information. (page 10)

Fourteen of PEBP's thirty-three employees have not received their annual security awareness training. Seven had no record of ever taking the training. During the course of the audit, we determined none of PEBP's three IT contractors received security awareness training as required by state security standards. Security awareness training helps ensure employees, consultants, and contractors are aware of their responsibilities in protecting state information. (page 10)

PEBP's system recovery and business continuity plan does not include sufficient information to enable its management to restore its critical services due to a system, application, or hardware malfunction. We determined PEBP's plan is not reviewed annually and has not been kept up to date. The plan references obsolete equipment and software inventory listings. Staff indicated the plan has been in place for some time and is outdated. PEBP must be able to continue to provide critical services should a situation occur that renders resources inaccessible. (page 12)

PEBP's data recovery procedures have not been adequately documented. Without adequate documentation, PEBP cannot develop comprehensive recovery procedures for each system, application, and associated data. (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

LEGISLATIVE BUILDING
401 S. CARSON STREET
CARSON CITY, NEVADA 89701-4747

RICK COMBS, *Director*
(775) 684-6800

LEGISLATIVE COMMISSION (775) 684-6800
NICOLE J. CANNIZZARO, *Senator, Chair*
Rick Combs, *Director, Secretary*

INTERIM FINANCE COMMITTEE (775) 684-6821
MAGGIE CARLTON, *Assemblywoman, Chair*
Cindy Jones, *Fiscal Analyst*
Mark Krmpotic, *Fiscal Analyst*

BRENDA J. ERDOES, Legislative *Counsel* (775) 684-6830
DANIEL L. CROSSMAN, Legislative *Auditor* (775) 684-6815
MICHEL J. STEWART, Research *Director* (775) 684-6825

Legislative Commission
Legislative Building
Carson City, Nevada

This report contains the findings, conclusions, and recommendations from our performance audit of the Public Employees' Benefits Program, 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 14 recommendations to improve the security of the agency's information systems. We are available to discuss these recommendations or any other items in the report with any legislative committees, individual legislators, or other state officials.

Respectfully submitted,

Daniel Crossman

Daniel L. Crossman, CPA
Legislative Auditor

January 31, 2020
Carson City, Nevada

Public Employees' Benefits Program Information Security Table of Contents

Public Employees' Benefits Program Information Security Table of Contents (continued)

Appendices

Introduction

Background

The Public Employees' Benefits Program (PEBP) is a state agency that is legislatively mandated to provide group health, life, and accident insurance for state and other eligible public employees. The first group insurance program in Nevada was created in 1963 and restructured into PEBP in 1999 as a result of Senate Bill 544.

PEBP currently administers various benefits and is responsible for designing and managing a quality health care program for approximately 43,000 primary participants and 27,000 covered dependents, totaling over 70,000 individuals. PEBP's mission is to provide employees, retirees, and their families with access to high quality benefits at affordable prices.

PEBP is governed by Chapter 287 of the Nevada Revised Statutes (NRS) and the Nevada Administrative Code (NAC). A 10-member Board oversees PEBP's operations. Nine Board members are appointed by the Governor, and the 10th member is the Director of the Department of Administration or his designee approved by the Governor. The Board appoints an Executive Officer to direct the day-to-day operations. The Board's purpose is to adopt regulations and policy for the agency. In fiscal year 2019, PEBP had 40 filled positions with 1 office located in Carson City. Operations include quality control, accounting, member services and eligibility, public information, and three positions dedicated to information technology (IT).

Funding for PEBP operations and insurance plans comes primarily from participant and employer contributions. PEBP submits its funding and operational requirements to the Legislature as part of the biennial budget. Upon approval, each state agency is assessed an amount to contribute toward both the active-employee and retiree health plans. For fiscal year 2019, PEBP had revenues of more than $376 million.

Scope and Objective

The scope of our audit included a review of the systems and practices in place during calendar year 2019 and included a review of security awareness training rosters from prior years. Our audit objective was to:

- Determine if PEBP 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 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.

Summary

The Public Employees' Benefits Program (PEBP) needs to strengthen its information system controls to ensure adequate protection of information systems and information processed therein. By taking action to address these control weaknesses, PEBP can better protect its physical resources, minimize security vulnerabilities, and ensure continuation of critical services.

Control weaknesses included: 1) inadequate security over computers and network devices, such as computers missing operating system and anti-virus updates; 2) not adequately managing users, including lack of account review and noncompliance with background check and security awareness training requirements; and 3) incomplete security related plans, such as lack of a current IT contingency plan and documentation of data recovery process.

Computers and Network Devices Had Inadequate Security

Some of PEBP's computers and network devices lacked adequate security. For example, many computers were missing critical operating system updates as well as current anti-virus definitions. Managing critical software updates is a vital process that can help alleviate many of the challenges of securing its computers. In addition, PEBP did not ensure laptops were properly configured with encryption software. Furthermore, improvements are needed to secure PEBP's multifunction device and wireless network.

Computers Were Missing Critical Operating System Updates

PEBP is not monitoring the status of operating system updates on its computers and laptops. The application, which PEBP utilizes to automate operating system updates, did not successfully deploy updates to 13 of the 20 computers and laptops we tested. This problem went undetected, as staff were not routinely verifying whether updates were installed successfully. Staff acknowledged additional training in the administration of the systems management application is needed to gain more familiarity with the system and its capabilities.

Software updates are important because they often include current security updates to address new vulnerabilities. Performing software updates is one of the most essential steps to protect information. Software updates can include security fixes, new or enhanced features, and better compatibility with different devices or applications. PEBP puts itself at risk by running software lacking current security updates. State security standards indicate maintaining IT systems with the latest available updates is a crucial part of protecting State IT systems.

Virus Protection Can Be Improved

PEBP is not ensuring its computers and laptops are current with anti-virus software. The application which automates anti-virus deployment was not successfully deploying virus definition updates to 24 of the 55 computers we tested. This problem went largely undetected as staff were not routinely verifying updates were installed successfully and were not familiar with the anti-virus management application.

With new viruses constantly being created, anti-virus programs must keep an updated database of virus types. This database includes a list of virus definitions the anti-virus software references when scanning files. By not maintaining its anti-virus software with current virus definitions, PEBP is unable to defend against new and emerging threats. State security standards require each agency to update virus protection software and definition files as new releases and updates become available.

Laptops Lacked Secure Configuration of Encryption Software

PEBP did not ensure 8 of its 11 laptops were properly configured with encryption software. These laptops are assigned to staff and are utilized on and offsite as needed. As laptops are mobile devices and can be easily stolen or lost, it is important for agencies to ensure they are adequately documented and protected.

State security standards indicate appropriate controls must be implemented to ensure the storage and transmission of an agency's sensitive data is protected. The most effective way to protect data is to encrypt it. On an encrypted drive, the data remains encrypted even if the drive is moved to a different system entirely. Encryption offers users the best protection against data theft or loss.

During the course of the audit, we also determined PEBP does not maintain adequate documentation of its mobile device agreements as they were not kept on file with the Information Security Officer or designee as required by state security standards. While PEBP has an existing new hire processing policy, mobile device agreements are not included in it. A mobile device agreement outlines responsibilities for both an agency manager and employee. These must be properly filled out, and list the approved applications to be installed and the data to be carried on the mobile device.

Improvements Are Needed to Secure a Multifunction Device

Improvements are needed to adequately secure PEBP's multifunction device. A multifunction device contains a hard drive that has the ability to store information when employees make copies, fax, scan, or print documents. This information must be erased after each job is completed. State security standards require overwrites after the completion of each print and scan job by default and a minimum three-pass erasure of any local storage medium. The setting on PEBP's multifunction device did not meet the state standard to ensure adequate overwrites of data in between jobs.

Additionally, staff indicated the multifunction device was used to forward received faxes to an internal print server, which then distributes the faxes into a folder on a network server. Staff were not aware state security standards require faxes to be received directly by the multifunction device itself, and not forwarded to a workstation or fax server.

Further, while current updates were available, the multifunction device's firmware was more than 3 years out of date. State security standards indicate the multifunction device administrator is responsible to periodically review it for firmware and software updates and apply these updates as needed.

A Wireless Access Point Was Not Configured Securely

PEBP has an improperly secured wireless access point for guests. The access point of a wireless network is where security configuration settings are enabled. PEBP's wireless network was password protected but lacked encryption. Staff indicated this access point had been operating in this condition for some time.

When a wireless network is run without encryption, all information sent over the unsecured wireless network can be viewed by anyone. Connecting to an open network potentially exposes a computer's communications to someone else on that wireless network. State security standards expect all wireless communications to be encrypted and password protected.

Recommendations

1. Obtain additional training to utilize the full capabilities of the operating system and anti-virus management applications to improve computer administration.
2. Develop procedures to routinely detect and correct failed computer operating system and anti-virus update installations.
3. Install and configure encryption software on laptops.
4. Update existing policies and procedures to ensure mobile device agreements are signed and kept on file.
5. Modify the overwrite settings of the multifunction device to ensure data is adequately erased.
6. Review the existing multifunction device configuration and determine a viable method to manage faxes.
7. Periodically review the multifunction device for firmware and software updates.
8. Configure encryption on the wireless access point.

Weaknesses Exist in User Management

Weaknesses include not performing periodic network maintenance as well as not routinely reviewing user access privileges in PEBP's applications. Furthermore, although PEBP had a procedure for revoking user access upon employee termination, it was not being followed. Lastly, IT contractor background checks were not conducted and staff did not always complete annual security awareness training.

Routine Account Maintenance Was Not Performed

Of PEBP's 110 network accounts, we identified 64 active user and service accounts that should be reviewed to determine their need. PEBP was disabling user accounts upon employee departure; however, it did not perform routine account maintenance to remove obsolete accounts.

User accounts are assigned to people to access network resources. Service accounts are built-in accounts that are used by automated systems services to access resources it needs to perform its activities. Service accounts are password-protected and often provide unrestricted access to the underlying resources, which is why attackers seek to gain access to them. In order to ensure service accounts are maintained, state security standards require that service account passwords are changed at least annually and not set to infinite expiration periods.

We identified 11 disabled network user accounts that could be removed. Staff indicated the disabled network user accounts were preserved for retention purposes, but we could not identify a history of this practice. In addition, staff acknowledged there was not a formal account review process in place. State security standards require user accounts be reviewed quarterly to ensure the continued need for access to a system, and that transferred or resigned users should be deleted.

Review of Critical Business Application Accounts Can Be Improved

PEBP is not routinely reviewing user access privileges in its five critical applications, and user access is not removed in a timely manner. These applications contain personal identifying information. During our analysis of the critical applications, we determined, although PEBP had established a procedure for revoking user access upon employee termination, it was not being followed. State security standards indicate termination of an employee must cause immediate revocation of all system and information access privileges.

PEBP could have identified users needing revocation if it had performed a quarterly review of accounts as required by state security standards. Staff indicated that because it was a small agency, there was no documentation to ensure that a review of user access occurred. Staff explained occasionally old user accounts that are no longer needed would be removed. Agencies are responsible for determining who may have access to protected information.

Building Access System Accounts Need Greater Review

Of PEBP's 53 accounts listed in the building access system, we found 2 accounts of former employees that were still active. The building access system is used to control access to PEBP's offices and server and telecommunications room. Although PEBP had a procedure outlining the process of disabling building access accounts, the process was not followed. Additionally, PEBP does not routinely audit its building access card system accounts.

State security standards indicate system managers shall reevaluate system access privileges granted to all users quarterly, at a minimum. Without conducting these routine reviews of user accounts, there is increased risk that former employees or other unauthorized persons may gain access to secure areas.

Staff were unable to provide a list of individuals with access to the server and telecommunications room. Further, they acknowledged that additional training in the administration of the building access system is needed to gain more familiarity with the application and its capabilities. State standards specify system managers must be able to produce a report of user IDs and access rights for their system upon demand, for the support of investigations and audits. Moreover, without a current user access list to the server and telecommunications room, it is not possible to determine if access is granted to authorized personnel only.

Contractor Background Checks Were Not Conducted

Background checks were not completed for PEBP's IT contractors. During our system account review, we identified three PEBP IT contractor accounts. We determined none of the contractors had background checks conducted as part of their hiring process, although PEBP conducted routine background checks on employees. These contractors had access to important information systems containing sensitive information.

Background checks investigate a candidate's background and identify potential hiring risk for safety and security reasons. State security standards indicate contractors and vendors who work for or provide IT services to the state are identified as sensitive and require background checks.

Security Awareness Training Was Not Always Completed

Fourteen of PEBP's thirty-three employees have not received their annual security awareness training. Seven had no record of ever taking the training. During the course of the audit, we determined none of PEBP's three IT contractors received security awareness training as required by state security standards. Security awareness training helps ensure employees, consultants, and contractors are aware of their responsibilities in protecting state information.

There is a greater risk users will not properly protect the information and information systems they have access to without completing such training. The Department of Administration, Enterprise IT Services Division recently implemented a new security awareness training system that has improved reporting capabilities. PEBP indicated it is taking steps to move to the new system.

State security standards indicate 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. Security awareness training must be reinforced at least annually.

Recommendations

9. Develop policies and procedures to ensure quarterly review of: 1) network user and service accounts; 2) critical business application user access; and 3) accounts within the building access system.
10. Follow the established procedure for revoking system access by disabling accounts immediately upon termination or a change in responsibilities of an employee or contractor.
11. Enhance the existing process to ensure IT contractors with access to PEBP's systems have background checks.
12. Update existing policy to define roles and responsibilities of individuals to monitor and ensure all employees, consultants, and IT contractors take initial and annual security awareness training.

Security-Related Plans Were Incomplete

PEBP does not have an effective process to ensure its security plans are reviewed and maintained. PEBP's system recovery and business continuity plan does not contain current information and instruction to enable it to continue its critical business services and operations. Further, PEBP does not define and document the testing of its data recovery procedures.

IT Contingency Plan Needs Attention

PEBP is not adhering to its system recovery and business continuity plan which states it will be reviewed annually and updated when major system changes are implemented. The plan references obsolete equipment and software inventory listings. Staff indicated the plan has been in place for some time and is outdated. An IT contingency plan should include sufficient information to enable its management to restore its critical services due to a system, application, or hardware malfunction. PEBP must be able to continue to provide critical services should a situation occur that renders resources inaccessible.

State security standards require agencies to update IT contingency plans at least annually and/or following any significant change to the computing environment. Contingency planning includes, but is not limited to, the documentation, plans, and policies and procedures required to restore critical IT functions.

Inadequate Testing and Documentation of Data Recovery Process

PEBP's data recovery procedures have not been adequately documented. Without adequate documentation, PEBP cannot develop comprehensive recovery procedures for each system, application, and associated data.

Although the IT backup and recovery policy outlines the basic steps for system and data recovery, it does not require scheduled testing of its data backup and recovery procedures. Staff explained there is no formal backup testing process although periodic restores from backups are needed and have been successful. No formal documentation of the restore results were prepared.

State security standards indicate data recovery test results should be documented and backup and recovery procedures shall be tested at least semiannually or more frequently for critical systems, applications and data. Further, state security standards indicate Information Security Officers are responsible for ensuring schedules and procedures for adequate system and data backup and recovery are in place.

Recommendations

13. Ensure the system recovery and business continuity plan is reviewed and kept up to date at least annually.
14. Update existing policies and procedures to define scheduling, testing, and documenting of the recovery processes at least semiannually.

Appendix A
Audit Methodology

To gain an understanding of the Public Employees' Benefits Program (PEBP), we interviewed management, staff and IT support staff. Through discussions, we gained a broad understanding of PEBP's information technology resources and how they are organized, maintained, and utilized. In addition, we reviewed generally accepted IT standards and guidelines from the State of Nevada and the National Institute of Standards and Technology. We also reviewed financial information, budgets, legislative committee minutes, and other information describing PEBP's activities. Furthermore, we documented and assessed internal controls over IT systems, users, and data resources.

We assessed internal security controls over 24 of 55 computers and tested to ensure they were protected with current application updates, laptop encryption, and mobile device agreement forms. Our testing of computers and laptop computers included an evaluation of application updates on devices that were available for testing. In addition, we tested a judgmental sample and reviewed the security of five of PEBP's critical applications to determine if access to sensitive data was authorized and appropriate.

To determine if only current employees had access to the network, we examined PEBP's network user population and compared users to active employee listings. In addition, we determined if all staff and IT contractors had conducted their annual security awareness training. Furthermore, we determined if PEBP was conducting background checks on staff and IT contractors who had access to sensitive information.

We assessed the server and telecommunications rooms housing PEBP's equipment for physical security including adequate access controls, and effective environmental controls. We also determined if PEBP’s building access card system that is used to grant access to restricted areas was being properly administered.

To determine if security controls over multifunction devices were adequate, we examined the multifunction device’s network configuration settings to verify if it meets state standards.

We evaluated PEBP’s IT contingency plan for the information systems that support its mission. For our review of disaster recovery, backup, and contingency plans, we assessed the existing documentation. We also examined PEBP’s efforts at ensuring appropriate backups and testing of backups were occurring. Finally, we assessed security configuration settings of PEBP’s wireless access points.

We assessed the full populations in our tests of server and telecommunication rooms access controls, network and application access controls, IT contractor background checks, security awareness training, multifunction devices, wireless access points, and network security.

For tests of computers and laptop computers security controls, we used nonstatistical audit sampling, which was the most appropriate and cost-effective methods 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 samples provide sufficient, appropriate audit evidence to support the conclusion in our report. Our judgmental selection of application access controls were made based on an assessment of key, critical applications. For these tests, we did not project the results to the population.

Our audit work was conducted from January to August 2019. 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 Public Employees' Benefits Program. On January 21, 2020, 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 17.

Contributors to this report included:

Shirlee Eitel-Bingham, CISA
Deputy Legislative Auditor

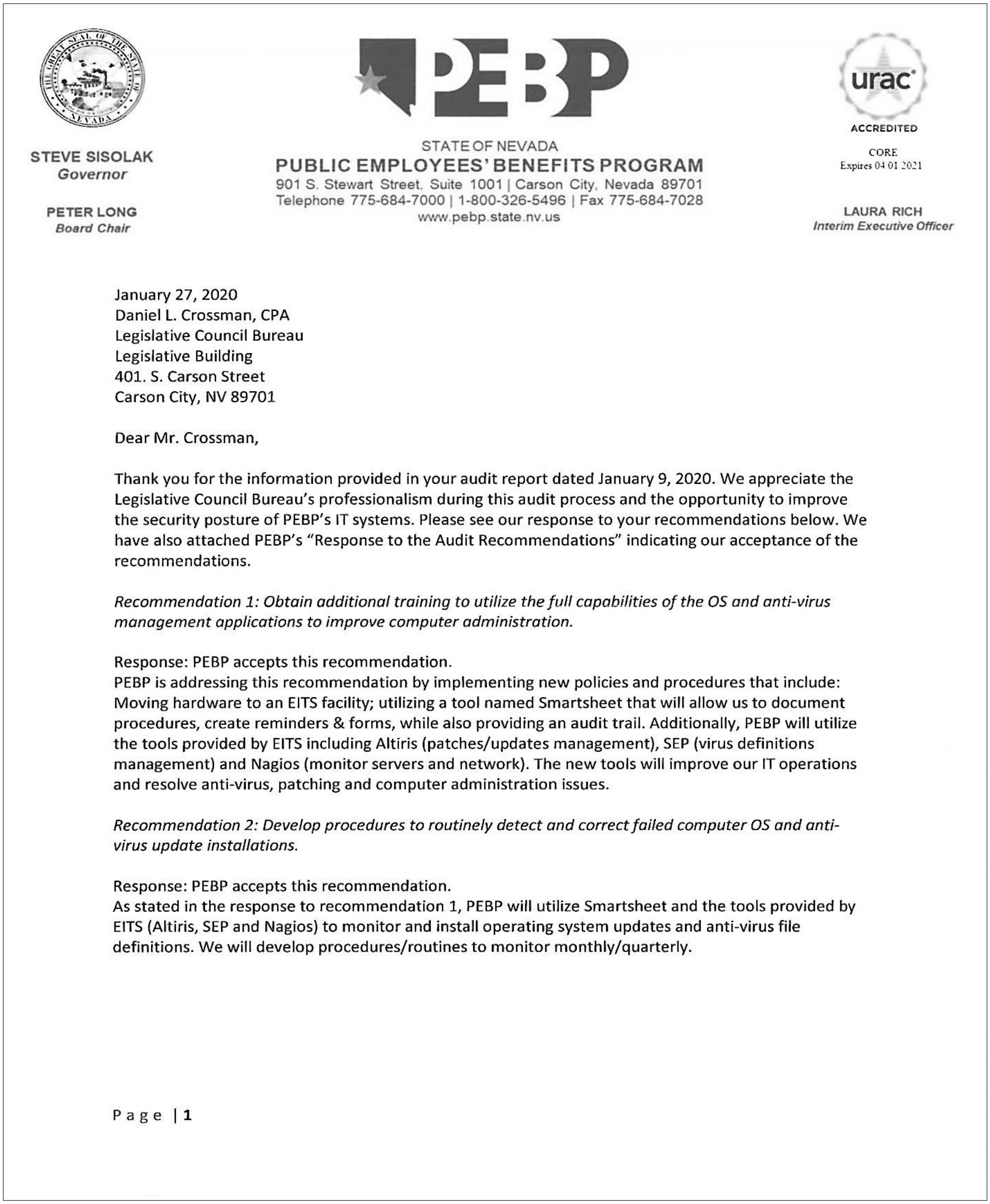
Sarah Gasporra, BBA
Deputy Legislative Auditor

S. Douglas Peterson, CISA, MPA
Information Systems Audit Supervisor

Shannon Ryan, CPA
Chief Deputy Legislative Auditor

Appendix B

Response From Public Employees' Benefits Program



STEVE SISOLAK
Governor

PETER LONG
Board Chair

PEBP

STATE OF NEVADA
PUBLIC EMPLOYEES' BENEFITS PROGRAM
901 S. Stewart Street, Suite 1001 | Carson City, Nevada 89701
Telephone 775-684-7000 | 1-800-326-5496 | Fax 775-684-7028
www.pebp.state.nv.us

urac®
ACCREDITED
CORE
Expires 04 01 2021

LAURA RICH
Interim Executive Officer

January 27, 2020
Daniel L. Crossman, CPA
Legislative Council Bureau
Legislative Building
401. S. Carson Street
Carson City, NV 89701

Dear Mr. Crossman,

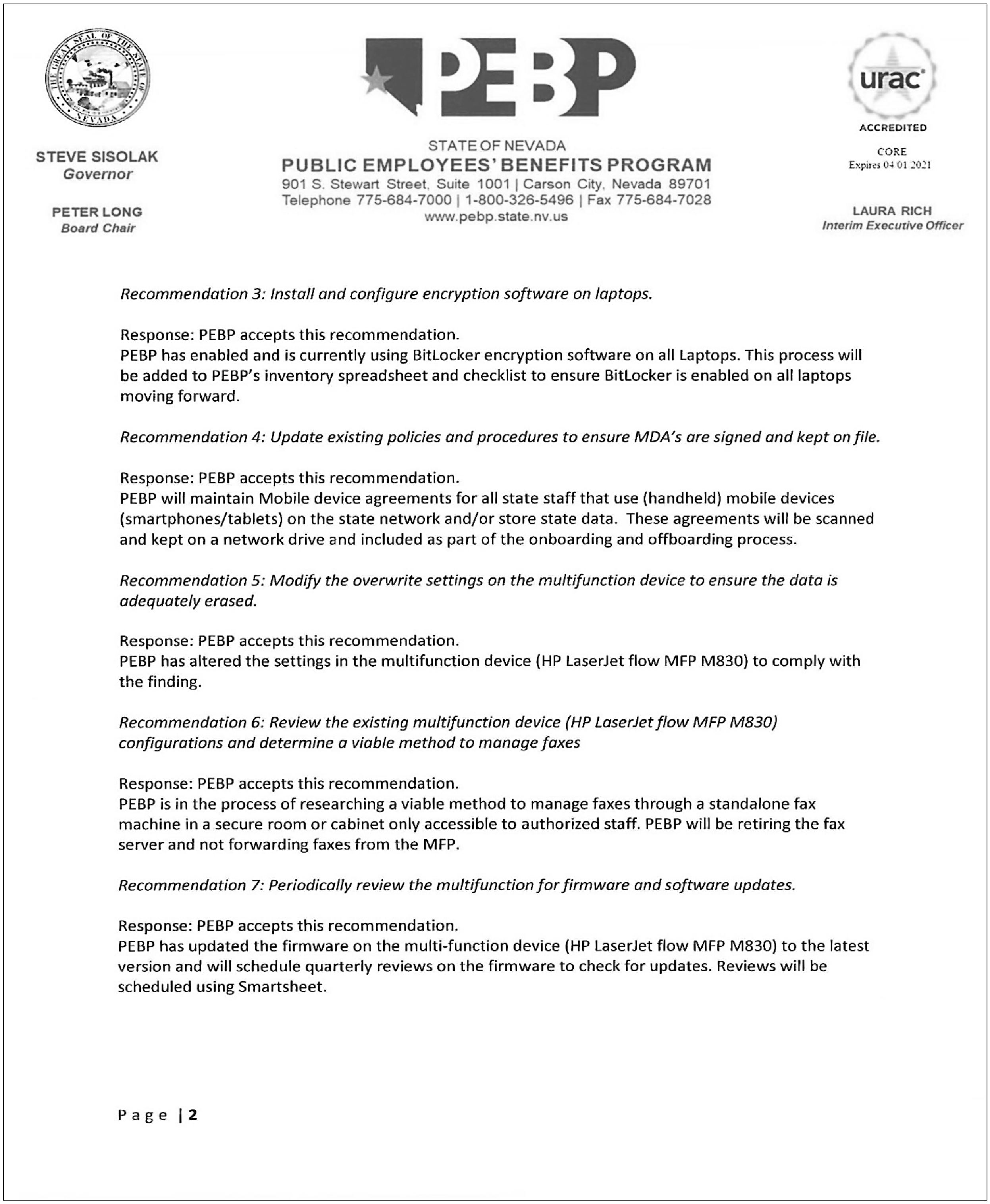
Thank you for the information provided in your audit report dated January 9, 2020. We appreciate the Legislative Council Bureau's professionalism during this audit process and the opportunity to improve the security posture of PEBP's IT systems. Please see our response to your recommendations below. We have also attached PEBP's "Response to the Audit Recommendations" indicating our acceptance of the recommendations.

Recommendation 1: Obtain additional training to utilize the full capabilities of the OS and anti-virus management applications to improve computer administration.

Response: PEBP accepts this recommendation.
PEBP is addressing this recommendation by implementing new policies and procedures that include: Moving hardware to an EITS facility; utilizing a tool named Smartsheet that will allow us to document procedures, create reminders & forms, while also providing an audit trail. Additionally, PEBP will utilize the tools provided by EITS including Altiris (patches/updates management), SEP (virus definitions management) and Nagios (monitor servers and network). The new tools will improve our IT operations and resolve anti-virus, patching and computer administration issues.

Recommendation 2: Develop procedures to routinely detect and correct failed computer OS and anti-virus update installations.

Response: PEBP accepts this recommendation.
As stated in the response to recommendation 1, PEBP will utilize Smartsheet and the tools provided by EITS (Altiris, SEP and Nagios) to monitor and install operating system updates and anti-virus file definitions. We will develop procedures/routines to monitor monthly/quarterly.



Recommendation 3: Install and configure encryption software on laptops.

Response: PEBP accepts this recommendation.
PEBP has enabled and is currently using BitLocker encryption software on all Laptops. This process will be added to PEBP's inventory spreadsheet and checklist to ensure BitLocker is enabled on all laptops moving forward.

Recommendation 4: Update existing policies and procedures to ensure MDA's are signed and kept on file.

Response: PEBP accepts this recommendation.
PEBP will maintain Mobile device agreements for all state staff that use (handheld) mobile devices (smartphones/tablets) on the state network and/or store state data. These agreements will be scanned and kept on a network drive and included as part of the onboarding and offboarding process.

Recommendation 5: Modify the overwrite settings on the multifunction device to ensure the data is adequately erased.

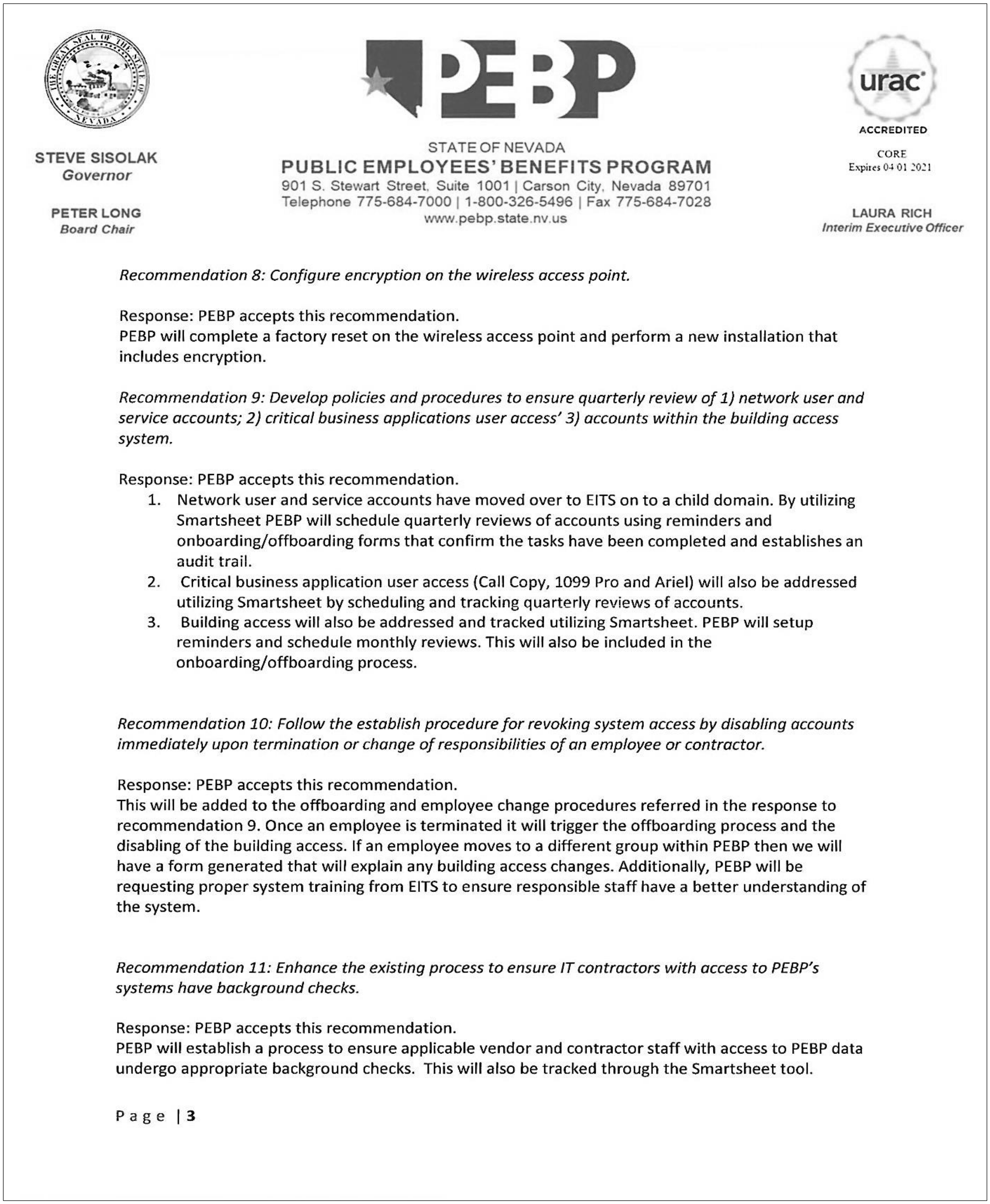
Response: PEBP accepts this recommendation.
PEBP has altered the settings in the multifunction device (HP LaserJet flow MFP M830) to comply with the finding.

Recommendation 6: Review the existing multifunction device (HP LaserJet flow MFP M830) configurations and determine a viable method to manage faxes

Response: PEBP accepts this recommendation.
PEBP is in the process of researching a viable method to manage faxes through a standalone fax machine in a secure room or cabinet only accessible to authorized staff. PEBP will be retiring the fax server and not forwarding faxes from the MFP.

Recommendation 7: Periodically review the multifunction for firmware and software updates.

Response: PEBP accepts this recommendation.
PEBP has updated the firmware on the multi-function device (HP LaserJet flow MFP M830) to the latest version and will schedule quarterly reviews on the firmware to check for updates. Reviews will be scheduled using Smartsheet.



STEVE SISOLAK
Governor

PETER LONG
Board Chair

STATE OF NEVADA
PUBLIC EMPLOYEES' BENEFITS PROGRAM
901 S. Stewart Street, Suite 1001 | Carson City, Nevada 89701
Telephone 775-684-7000 | 1-800-326-5496 | Fax 775-684-7028
www.pebp.state.nv.us

urac
ACCREDITED
CORE
Expires 04 01 2021

LAURA RICH
Interim Executive Officer

Recommendation 8: Configure encryption on the wireless access point.

Response: PEBP accepts this recommendation.
PEBP will complete a factory reset on the wireless access point and perform a new installation that includes encryption.

Recommendation 9: Develop policies and procedures to ensure quarterly review of 1) network user and service accounts; 2) critical business applications user access' 3) accounts within the building access system.

Response: PEBP accepts this recommendation.

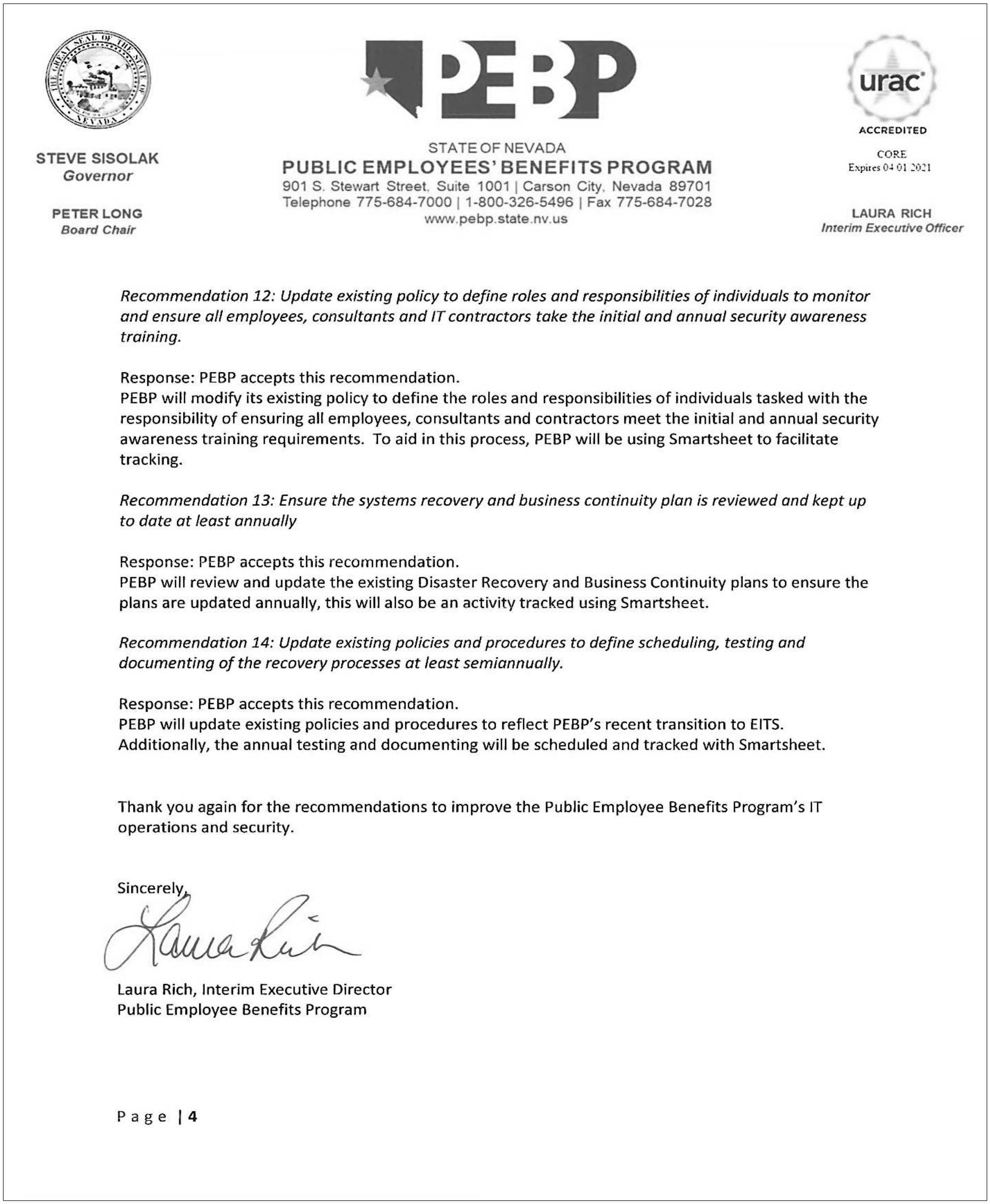
1. Network user and service accounts have moved over to EITS on to a child domain. By utilizing Smartsheet PEBP will schedule quarterly reviews of accounts using reminders and onboarding/offboarding forms that confirm the tasks have been completed and establishes an audit trail.
2. Critical business application user access (Call Copy, 1099 Pro and Ariel) will also be addressed utilizing Smartsheet by scheduling and tracking quarterly reviews of accounts.
3. Building access will also be addressed and tracked utilizing Smartsheet. PEBP will setup reminders and schedule monthly reviews. This will also be included in the onboarding/offboarding process.

Recommendation 10: Follow the establish procedure for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor.

Response: PEBP accepts this recommendation.
This will be added to the offboarding and employee change procedures referred in the response to recommendation 9. Once an employee is terminated it will trigger the offboarding process and the disabling of the building access. If an employee moves to a different group within PEBP then we will have a form generated that will explain any building access changes. Additionally, PEBP will be requesting proper system training from EITS to ensure responsible staff have a better understanding of the system.

Recommendation 11: Enhance the existing process to ensure IT contractors with access to PEBP's systems have background checks.

Response: PEBP accepts this recommendation.
PEBP will establish a process to ensure applicable vendor and contractor staff with access to PEBP data undergo appropriate background checks. This will also be tracked through the Smartsheet tool.



STEVE SISOLAK
Governor

PETER LONG
Board Chair

PEBP

STATE OF NEVADA
PUBLIC EMPLOYEES' BENEFITS PROGRAM
901 S. Stewart Street, Suite 1001 | Carson City, Nevada 89701
Telephone 775-684-7000 | 1-800-326-5496 | Fax 775-684-7028
www.pebp.state.nv.us

urac®
ACCREDITED
CORE
Expires 04 01 2021

LAURA RICH
Interim Executive Officer

Recommendation 12: Update existing policy to define roles and responsibilities of individuals to monitor and ensure all employees, consultants and IT contractors take the initial and annual security awareness training.

Response: PEBP accepts this recommendation.
PEBP will modify its existing policy to define the roles and responsibilities of individuals tasked with the responsibility of ensuring all employees, consultants and contractors meet the initial and annual security awareness training requirements. To aid in this process, PEBP will be using Smartsheet to facilitate tracking.

Recommendation 13: Ensure the systems recovery and business continuity plan is reviewed and kept up to date at least annually

Response: PEBP accepts this recommendation.
PEBP will review and update the existing Disaster Recovery and Business Continuity plans to ensure the plans are updated annually, this will also be an activity tracked using Smartsheet.

Recommendation 14: Update existing policies and procedures to define scheduling, testing and documenting of the recovery processes at least semiannually.

Response: PEBP accepts this recommendation.
PEBP will update existing policies and procedures to reflect PEBP's recent transition to EITS. Additionally, the annual testing and documenting will be scheduled and tracked with Smartsheet.

Thank you again for the recommendations to improve the Public Employee Benefits Program's IT operations and security.

Sincerely,

Laura Rich

Laura Rich, Interim Executive Director
Public Employee Benefits Program

Public Employees' Benefits Program's Response to Audit Recommendations

	Recommendations	Accepted	Rejected
1.	Obtain additional training to utilize the full capabilities of the operating system and anti-virus management applications to improve computer administration	X	
2.	Develop procedures to routinely detect and correct failed computer operating system and anti-virus update installations	X	
3.	Install and configure encryption software on laptops	X	
4.	Update existing policies and procedures to ensure mobile device agreements are signed and kept on file	X	
5.	Modify the overwrite settings of the multifunction device to ensure data is adequately erased	X	
6.	Review the existing multifunction device configuration and determine a viable method to manage faxes	X	
7.	Periodically review the multifunction device for firmware and software updates	X	
8.	Configure encryption on the wireless access point	X	
9.	Develop policies and procedures to ensure quarterly review of: 1) network user and service accounts; 2) critical business application user access; and 3) accounts within the building access system	X	
10.	Follow the established procedure for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor	X	
11.	Enhance the existing process to ensure IT contractors with access to PEBP's systems have background checks	X	
12.	Update existing policy to define roles and responsibilities of individuals to monitor and ensure all employees, consultants, and IT contractors take initial and annual security awareness training	X	
13.	Ensure the system recovery and business continuity plan is reviewed and kept up to date at least annually	X	
14.	Update existing policies and procedures to define scheduling, testing, and documenting of the recovery processes at least semiannually	X	
	TOTALS	14	