STEVE SISOLAK
*Governor*

LAURA FREED
*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

ACCREDITED
CORE
Expires 04/01/2021

LAURA RICH
*Executive Officer*

# AGENDA ITEM

☒ Action Item

□ Information Only

**Date:** January 28, 2021

**Item Number:** VIII

**Title:** Legislative Counsel Bureau IT Audit – Corrective Action Plan

## Summary

In January 2019, PEBP was notified by the Legislative Counsel Bureau (LCB) Audit Division that it would be performing an Information Technology and Security audit of the agency.

On January 9, 2020, the LCB provided the agency with an initial draft of the final findings to which PEBP was required to submit a written response indicating acceptance or disagreement. A corrective action plan was developed, approved by the Board and implemented since that time.

In October 2020, PEBP was notified of an addendum to the original audit that included four additional items to be addressed. These four new items were not included on the original LCB audit report due to security risks that could result from making these findings public prior to the appropriate security measures being implemented. These concerns have since been addressed.

On January 14, 2021 PEBP accepted these additional findings during the Legislative Commission Audit Subcommittee meeting. As a result, PEBP must provide an initial 60-day corrective action plan followed by a subsequent six-month status report. PEBP has developed the proposed corrective action plan to future-proof the concerns identified in the audit.

## Report

See Attachment A

# Attachment A

*Recommendation 15: Develop and maintain an agency-wide server asset lifecycle plan.*

Response:
PEBP accepts this recommendation.
PEBP is eliminating all agency-owned servers and will instead utilize third-party (EITS) servers and services to support its various programs.

**Corrective Action:**
**PEBP will create a new policy and procedure that reflects its ongoing efforts to monitor and manage these hosted systems utilizing existing EITS policies, standards and procedures. Specifically, policy will require that the agency Chief Information Officer review annually with EITS all servers to ensure appropriate lifecycle planning (and any required remediation) is performed annually.**

*Recommendation 16: Develop policies and procedures to routinely verify servers and receiving operating system and database software critical updates and ensure they are successfully installed.*

Response:
PEBP accepts this recommendation.
PEBP is eliminating all agency-owned servers and will instead utilize third-party (EITS) servers and services to support its various programs.

**Corrective Action:**
**PEBP will create a new policy and procedure that reflects its ongoing efforts to monitor and manage these hosted systems utilizing existing EITS policies, standards and procedures. Specifically, policy will require that the agency Information Security Officer and Chief Information Officer review annually with EITS all servers, desktops, databases and other systems to ensure appropriate patching (and any required remediation) is performed at least annually.**

*Recommendation 17: Develop policies and procedures to ensure vulnerability scanning of servers is conducted at least annually to assist in identifying areas of risk.*

Response:
PEBP accepts this recommendation.
PEBP is eliminating all agency-owned servers and will instead utilize third-party (EITS) servers and services to support its various programs.

**Corrective Action:**
**PEBP will create a new policy and procedure that reflects its ongoing efforts to monitor and manage these hosted systems utilizing existing EITS policies, standards and procedures. Specifically, policy will require that the agency Information Security Officer and Chief Information Officer review annually with EITS all servers to ensure appropriate scanning (and any required remediation) is performed annually.**

*Recommendation 18: Ensure existing server inventory and password management software is maintained.*

Response:
PEBP accepts this recommendation.
PEBP will utilize an existing system that maintains this critical and confidential information.

**Corrective Action:**
**PEBP has an existing system (KeePass) that will be utilized and routinely monitored to ensure integrity and accuracy of this critical and confidential data, and this procedure will be updated into policy to be reviewed at least annually.**