AGENDA ITEM

|X| Action Item

|☐| Information Only

Date:　　　　　March 31, 2020

Item Number:　X

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. Throughout the year, PEBP staff have been working diligently to assist the auditors and have collected all requested data and information required by the auditors to perform this function. 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.

The report indicates PEBP's need to strengthen information system controls to better protect its physical resources, minimize security vulnerabilities and ensure continuation of critical services. PEBP accepted all 14 findings and provided an initial plan on how the agency intended to rectify the deficiencies identified in the report.

The findings and associated responses were presented to and accepted by the Legislative Commission's Audit Subcommittee on February 18, 2020. PEBP must provide an initial 60-day corrective action plan followed by a subsequent six-month status report due at a later date.

REPORT

See Attachment A

March 31, 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 and the opportunity to present on PEBP's responses to the Legislative Audit Subcommittee on February 18, 2020. We appreciate the Legislative Council Bureau's professionalism during this audit process and believe the audit was a valuable experience for PEBP.

Attached is PEBP's initial response to the audit recommendations, indicating PEBP's acceptance of the recommendations as well as the updates to actions that have been taken since.

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

Sincerely,

Laura Rich, Executive Officer
Public Employee Benefits Program

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 Update:
PEBP plans to finalize the hardware migration to EITS and utilize their tools (Altiris, SEP and Nagios) on servers and desktops to produce scheduled reports that will ensure proper patching and system administration. PEBP has purchased and installed software (Smartsheet) which will allow PEBP to document, track and ensure these procedures are being followed and provide an audit trail.

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 Update:
PEBP has started using the tools stated in recommendation 1 and is in the process of building reports, procedures and routines to monitor and ensure proper patching and updates are performed.

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 Update:
PEBP has and installed and configured BitLocker encryption software on all laptops. All new laptops will have BitLocker enabled/installed and utilized.

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 Update:
PEBP has ensured all signed mobile device agreements are stored in the appropriate network folder. This will be added to the employee onboarding and offboarding process and will be reflected in PEBP's Personnel Security Policy.

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 Update:
The Multifunction device was updated accordingly 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 Update:
PEBP has purchased and installed a secure cabinet and a standalone fax machine that is only accessible by authorized staff. PEBP has requested EITS Telecom staff move existing fax lines to ensure we fully satisfy and comply with this recommendation.

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.

Recommendation Update:
PEBP has updated the firmware on all MFD's and printers in the office and will utilize Smartsheet to create reminders to check for future firmware updates.

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 Update:
This will be completed by March 31, 2020.

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 Update:
PEBP is in the process of creating work flow reminders and forms in Smartsheet to facilitate scheduled reviews of Active Directory accounts, network service accounts, critical business applications, as well as managing 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 Update:
This will be included as part of the offboarding process and will be formalized by utilizing Smartsheet. A separate formal process will be established to address staff who move between groups within the agency. PEBP will request and schedule training from EITS staff to ensure responsible staff have a complete 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.

Recommendation Update:
PEBP will perform background checks on all applicable vendor and contractor staff with access to PEBP data. Applicable vendor and contractor staff as defined per NRS 239B and the State of NV

Information Security Committee Standard S.3.04.01 "Personnel Security". PEBP has contacted the Division of Human Resource Management for guidance on this matter.

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 Update:
PEBP's Executive Assistant is currently responsible for tracking this information using an Excel spreadsheet. This will be upgraded to utilize Smartsheet with automated reminders to track annual training and be part of the onboarding process for the initial training.

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 Update:
PEBP is in the process of reviewing and updating the Disaster Recovery and Business Continuity plans that will include semiannual testing.

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 semiannual testing and documenting will be scheduled and tracked with Smartsheet.

Recommendation Update:
As mentioned in recommendation 13, PEBP will schedule, test, document and update the Disaster Recovery and Business Continuity Plans at least semiannually. This will be tracked in Smartsheet.