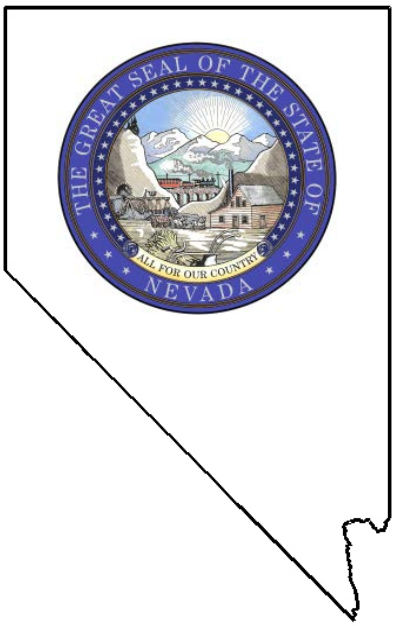
STATE OF NEVADA

Performance Audit – Addendum

Public Employees' Benefits Program

Information Security – Servers
LA20-13A

Operating System and Database Application Software



Legislative Auditor
Carson City, Nevada

STATE OF NEVADA
LEGISLATIVE COUNSEL BUREAU
LEGISLATIVE BUILDING
401 S. CARSON STREET
CARSON CITY, NEVADA 89701-4747
Fax No.: (775) 684-6600

Legislative Commission
Legislative Building
Carson City, Nevada

This report addendum LA20-13A contains supplemental findings, conclusions, and recommendations from our performance audit of the Public Employees' Benefits Program, Information Security (LA20-13). We issued that report on February 18, 2020. The audit was conducted pursuant to the ongoing program of the Legislative Auditor as authorized by the Legislative Commission, and was made pursuant to provisions of NRS 218G.010 and 218G.350.

An addendum to report LA20-13 was necessary because security vulnerabilities existed in certain information systems within the Public Employees' Benefits Program. Providing details regarding those vulnerabilities, at the time we made the original report public, would have unnecessarily exposed those information security weaknesses. Since the agency has performed sufficient corrective actions, we are issuing this addendum as a supplement to our original report. Readers are encouraged to refer to report LA20-13 and this report addendum to gain a complete and comprehensive understanding of the audit's scope and objective, findings, recommendations, and methodology.

This addendum includes four additional recommendations to improve the security of the agency's servers. 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

November 5, 2020
Carson City, Nevada

Addendum to Audit Report LA20-13

Server Software Lacked Critical Security Updates

Many of the Public Employees' Benefits Program's (PEBP) servers had critical security vulnerabilities due to outdated and unsupported software. PEBP did not ensure that operating systems and database application software were upgraded to supported versions in a timely manner. Knowing key dates in a software asset lifecycle plan ensures an organization makes informed decisions about when to upgrade or make other changes to its software. Without proper software upgrade planning, PEBP compromises security, performance, and overall efficiency.

We determined all servers were not current with Microsoft Windows operating system security updates. PEBP's designated server for update deployment was not issuing Windows operating system updates successfully. Furthermore, updates were not routinely verified for successful installation. In addition, we determined adequate documentation of procedures for administering the server was not maintained. State security standards require agencies to implement a process to deploy critical or actively exploitable security patches.

Further, we determined one server was running outdated Windows operating system software as well as outdated database software. There were no current security updates available, as the vendor no longer supported the operating system and database versions of software installed. State security standards indicate operating systems or commercial applications that have reached end-of-support from the vendor must be upgraded to a currently supported version.

PEBP was also not conducting vulnerability scanning on its servers. PEBP could have identified outdated software and security update issues earlier had they performed vulnerability scanning and maintained a software inventory. Conducting scans on a frequent basis identifies and prioritizes vulnerabilities. State Information Security Program Policies require all systems have vulnerability scans to identify security threats at least annually.

Some Servers Lacked Virus Protection Software

Controls over virus protection for PEBP's servers were deficient. The server, which automates antivirus deployment, was not updating 9 of the 22 Windows servers. Four did not have the antivirus client software installed and five did not have current antivirus updates. In addition, the system administrator was not routinely verifying antivirus updates were successfully installed and did not have documentation of procedures for administering the server. State security standards state each agency shall update virus protection software and definition files as new releases and updates become available.

Linux Servers Lacked Oversight

Some of the agency's Linux servers were not adequately maintained. Of the nine Linux servers at PEBP, we determined only three were running a current distribution of Linux. However, the system administrator could not identify the distribution or version of the remaining Linux servers. Through discussions with staff as well as our observations, we determined the system administrator had not maintained adequate password documentation nor sufficient server documentation to ensure server maintenance was occurring.

Recommendations

1. Develop and maintain an agency-wide server software asset lifecycle plan.
2. Develop policies and procedures to routinely verify servers are receiving operating system and database software critical updates and ensure they are successfully installed.
3. Develop policies and procedures to ensure vulnerability scanning of servers is conducted at least annually to assist in identifying areas of risk.
4. Ensure existing server inventory and password management software is maintained.

Actions Taken by the Agency to Resolve the Security Vulnerabilities

After the security vulnerabilities were identified in the servers, the agency established a plan to mitigate them. The plan involved utilizing the Division of Enterprise Information Technology Services' software update and antivirus management services, as well as a full documentation and system review of PEBP's information technology environment.

Beginning in February 2020, we conducted monthly meetings to obtain status reports and monitor the progress of system and software upgrades. We continued to monitor PEBP's progress until successful upgrading, patching, or decommissioning of all servers was complete.

Methodology

To assess the logical security controls of all of PEBP's servers, we tested to ensure they were protected with current antivirus, operating system, and database software updates. Based on the results of this test work and identifying outdated software, we conducted monthly meetings with PEBP's IT staff and management regarding resolution of these issues.

Our audit work was conducted from January 2019 to August 2020. 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.

Statutorily Required Corrective Action and Follow-Up
The 4 recommendations on page 3 are in addition to the 14 issued in the original report LA20-13 and are subject to the corrective action and follow-up requirements outlined in NRS 218G.250 and 218G.270. The Agency's 60-day plan for corrective action on the four recommendations in this addendum is due on April 9, 2021 and the 6-month report on the status of audit recommendations is due on October 9, 2021.

In accordance with NRS 218G.230, we furnished a copy of our preliminary report addendum to the Public Employees' Benefits Program. On October 19, 2020, we met with agency officials to discuss the results of the audit and requested a written response to the preliminary report addendum. That response is included on page 6.

Contributors to this report included:

Shirlee Eitel-Bingham, CISA
Deputy Legislative Auditor

Sarah Gasporra, BA
Deputy Legislative Auditor

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

Shannon Riedel, CPA
Chief Deputy Legislative Auditor

Response From the Public Employees' Benefits Program

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

urac ACCREDITED
CORE
Expires 04/01/2021

LAURA RICH
Executive Officer

October 29, 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 October 9, 2020. We appreciate the Legislative Council Bureau's professionalism during this audit process and the opportunity to improve the security of PEBP's IT systems. Please see the agencies' responses to your recommendations below. We have also attached PEBP's "Response to the Audit Recommendations" indicating our acceptance of the recommendations.

Recommendation 1: Develop and maintain an agency-wide server software asset lifecycle plan.

Response: PEBP accepts this recommendation.
In response to this finding, PEBP has developed an asset lifecycle plan and has implemented a system to track and monitor replacement schedules. Additionally, PEBP has purchased new servers to replace existing servers with past due end-of-life replacement dates.

Recommendation 2: Develop policies and procedures to routinely verify servers are receiving operating system and database software critical updates and ensure they are successfully installed.

Response: PEBP accepts this recommendation.
PEBP has taken appropriate measures to ensure routine updates are managed automatically through Enterprise IT Services (EITS) and that proper oversight occurs on the agency level. Policies and Procedures will be updated accordingly.

Recommendation 3: 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.
In coordination with EITS, PEBP has already taken appropriate measures to reduce server vulnerability. Some existing servers were decommissioned and transitioned to EITS while other older servers have been replaced.

Recommendation 4: Ensure existing server inventory and password management software is maintained.

Response: PEBP accepts this recommendation.

As a result of this finding, PEBP IT staff have taken proper measures to ensure this recommendation is accomplished both externally through existing EITS processes and internally via a newly implemented tracking and oversight system. Additionally, the appropriate updates to agency policies and procedures will be made.

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

Sincerely,

X 

Laura Rich
Executive Officer, Public Employees' Benefits Progr...
Signed by: 8d3ae9d7-40c6-491d-85c0-7ec0133f30a0

Laura Rich, Executive Director
Public Employee Benefits Program

Public Employees' Benefits Program Response to Addendum Recommendations

	Recommendations	Accepted	Rejected
1.	Develop and maintain an agency-wide server software asset lifecycle plan	X	
2.	Develop policies and procedures to routinely verify servers are receiving operating system and database software critical updates and ensure they are successfully installed	X	
3.	Develop policies and procedures to ensure vulnerability scanning of servers is conducted at least annually to assist in identifying areas of risk	X	
4.	Ensure existing server inventory and password management software is maintained	X	
	TOTALS	4	