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)