



Oregon

Kate Brown, Governor

Public Employees Retirement System

Headquarters:

11410 S.W. 68th Parkway, Tigard, OR

Mailing Address:

P.O. Box 23700

Tigard, OR 97281-3700

(503) 598-7377

TTY (503) 603-7766

www.oregon.gov/pers

September 7, 2018

The Honorable Senator Chuck Riley, Co-Chair
The Honorable Representative Nancy Nathanson, Co-Chair
Interim Joint Committee on Information Management and Technology
900 Court Street NE
H-178 State Capitol
Salem, OR 97301-4048

Dear Co-Chairpersons:

Nature of the Request

PERS has been asked to report to the Interim Joint Committee on Information Management and Technology on the status of the progress of implementation around the following topics:

1. Development and implementation of an industry standard Cyber Security Program, including defining the long-term maintenance, operation, staffing and funding plans for the program;
2. Development and implementation of industry standard Disaster Recovery and Business Continuity Programs.

Agency Action

PERS continues to work with the Office of the State Chief Information Officer (OSCIO) on the planning and implementation of these initiatives and will report on progress as requested.

INFORMATION SECURITY PROGRAM DEPLOYMENT PROJECT

Background

PERS was directed to develop and implement an industry standard Information Security Program, including defining the long-term operation, maintenance, staffing and funding plans for the program. Once completed, the Information Security Program is to be independently assessed by a third-party vendor with the findings of that assessment reported to the Legislature during the 2019 legislative session.

In response to communications from the Governor's Chief of Staff and a subsequent joint memo from the Legislative Fiscal Office (LFO) and OSCIO in April 2016, PERS contracted with HP Enterprise (now DXC) to support remediation activities and complete initial planning for the PERS Information Security program as part of the Information Security Enhancements project completed in June 2017. This included development of the funding request and draft business case for the PERS Cybersecurity Program (2017-2019 biennium, Policy Package 101), which was approved. Through the passage of Senate Bill 90 2017 and ORS 276A, Cybersecurity for the State of Oregon was unified under the Enterprise Security Office (ESO) and the staffing positions approved through Package 101 were transferred to ESO.

The PERS Information Security Program Deployment project includes the remaining work to fully establish the program and transition to ongoing security operations. This includes program staffing, funding, policies and standards development, implementation of the Information Security Training and Awareness program and completion of the remaining critical security remediation activities related to the April 7, 2016 Joint LFO/OSCIO memo on PERS information security.

Upon completion of these deliverables, PERS (with guidance from ESO) will secure a third-party vendor to perform a security assessment and provide a report to the OSCIO and legislature.

Status Update since May 2018

- PERS filled the new Information Security and Risk officer position which was approved in the last Ways and Means legislation for the February 2018 session. This position will centralize accountability for information security, business continuity, disaster recovery, and enterprise risk management within the agency.
- PERS completed a Project Management Plan and a detailed project schedule which were reviewed for completeness by OSCIO. The Conditional Approval Memorandum for the project was issued by the OSCIO on July 17, 2018.
- An addendum to the Conditional Approval Memorandum was issued August 3, 2018, to further clarify the procurement process for the project.
- In collaboration with ESO, PERS finalized the scope for the Information Security Program Development and Implementation, which includes the following:
 - Develop an Information Security Program Plan
 - Review and update the Agency's Information Security Plan
 - Review and update the Agency's Information Security Incident Response Plan
 - Develop the Agency's Information Security Program Key Performance Measures (KPIs)
 - Review and update the Agency's core Information Security Policies, Standards, and Procedures
 - Review and define key staffing to oversee core Information Security processes
 - Review and update the Agency's Software Development Life Cycle (SDLC) Plan
 - Develop the Agency's Information Security Training and Awareness Plan
- In addition to program development, PERS made significant progress in executing on the remediation activities
 - Access Control and Authentication: All access control policies and standards are complete and published. The multi-factor authentication (MFA) solution has been selected and is in procurement. The 7,000 test user accounts/shared access accounts are in the process of being deleted and named test accounts created for software development activities.
 - Log Management/Incident Monitoring: Collaborating with ESO to provide ongoing monitoring and alerting on PERS information system logs.
 - Security Policies and Procedures: The governance model has been implemented and the security policies are being revised in support of the remediation activities and the overall program lifecycle.
 - Network Security/Segmentation: Purchased the micro segmentation infrastructure (i.e. VMware NSX) and deployed the external network zones, also known as DMZs in preparation for application (Host) deployment.

- Software Development: A cross functional working group is tasked with evaluating the agency's System Development Life Cycle and establishing a Secure Development Lifecycle (SDL), including coding practices, and code analysis tools and procedures.
- Technical Controls: Currently performing a gap analysis for technical controls such as data loss prevention (DLP) and data privacy.
- Training Program: The governance model for the agency training and awareness program, in alignment with the enterprise program, is being drafted. The target date for completion is October 2, 2018. Supplemental application development security training has been purchased and preparations for rollout to development staff are underway. Internal agency monthly awareness campaigns have been implemented.
- To assist with the continuing Information Security program development activities, and ensure that PERS is able to operate its program by the end of the 2017-2019 biennium, PERS respectfully requests the establishment of a security analyst position effective January 2, 2019.
- Upon the recommendation of this committee, PERS is prepared to submit a request for the December 2018 Emergency Board for the information security analyst position.

CONTINUITY MANAGEMENT PROGRAM - DEPLOYMENT PROJECT (CMP)

Background:

PERS had been directed to develop and implement industry-standard Business Continuity and Disaster Recovery Programs with funding approved in Policy Packages 803 and 804 of SB 5534 (2017). PERS is working on the development of a comprehensive project plan for its overall Continuity Management Program (CMP). One of the cornerstones of our CMP is the current PERS Business Continuity Plan (BCP). Another crucial area that fits into the overall framework of this project is establishing a Disaster Recovery (DR) Program. PERS is working to deploy a program that includes various components which need to be in place to ensure this agency's core functions can continue:

- Develop a new Continuity of Operations Plan (COOP)
- Contracting with a third-party vendor for consultation, program development and implementation and program certification
- Disaster Recovery Planning and Program Development
- Staff and Manager Training Plan
- Program testing and exercises
- Development of Metrics (so we know if we are successful)
- Updates to Annual Review Process (to ensure plans remain current)

Status Update since May 2018

- In our previous update, PERS reported that the Department of Administration Services (DAS) issued a new state policy directing agencies to create and implement a COOP, superseding the state's earlier policy on Business Continuity Planning. Since that report, PERS completed its evaluation of the impact of the COOP development to the current project scope. In coordination with OSCIO, the project scope statement was finalized and accepted.

- The program name (and related project name) was updated to be more inclusive and overarching of BCP, COOP and Disaster Recovery components - now the “Continuity Management Program.”
 - PERS submitted an initial draft of its COOP Plan to the Governor’s office by their July 1st deadline. Input will be provided to PERS, and an updated COOP must be re-submitted by December 31, 2018.
- A procurement was conducted in collaboration with DAS and OSCIO to hire a third-party vendor to assist PERS in developing and implementing an industry standard Continuity Management Program (CMP). A contract was awarded to Deloitte and PERS finalized the Statement of Work (SOW). This work will be completed within the current biennium in two primary phases:
 - Phase I - Analysis and planning (this will inform and help PERS finalize its project schedule and project management plan).
 - Phase II - Implementation and execution.
- PERS conducted a tabletop test in August of a pension roll re-run with its internal incident response team in coordination with Oregon State Treasury. This exercise was concluded with an after action report process to document lessons learned for future exercises.
- PERS hired a new Information Security and Risk officer who is now directly managing this function as a long-term agency program.
- To assist with the Continuity Management program development activities, and ensure that PERS is able to operate its program by the end of the 2017-2019 biennium, PERS respectfully requests the establishment of a continuity and disaster recovery analyst position, effective January 2, 2019
- Upon the recommendation of this committee, PERS is prepared to submit a request for the December 2018 Emergency Board, for the continuity and disaster recovery analyst position.

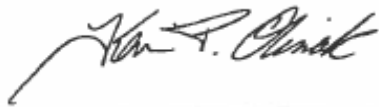
Action Requested

Discussion, recommendation and acknowledge receipt of the report.

Legislation Affected

This report reflects Budget Note directives as approved in Senate Bill 5534(2017) and additional directives from the Legislative Fiscal Office.

Respectfully,



Kevin Olineck

Director

Oregon Public Employees Retirement System