# MEMORANDUM

Legislative Fiscal Office
900 Court St. NE, Room H-178
Salem, Oregon 97301
Phone 503-986-1828
FAX 503-373-7807

| | |
|---|---|
| **To:** | Joint Legislative Committee on Information Management and Technology |
| **From:** | Robert L. Cummings, Principal Legislative Analyst (IT) |
| | John Borden, Principal Legislative Analyst |
| **Date:** | February 12, 2016 |
| **Subject:** | PERS Disaster Recovery and Business Continuity Planning - Budget Note Report |
| | LFO Analysis and Recommendations |

**Agency Request:** During the 2015 legislative session within HB 5034 - Policy Option Package (POP) #105, the Public Employees Retirement System (PERS) made a 2015-17 request for Other Funds expenditure limitation in the amount of $1,581,000, to upgrade its existing Disaster Recovery (DR) and Business Continuity Planning (BCP) environment. This amount included $555,200 for "services & supplies Other Funds limitation" and $1,026,000 in "capital outlay Other Funds limitation." Specifically, POP #105 included three key components: 1) Disaster Recovery Planning & Infrastructure - $881,000; 2) Virtual Desktop Environment - $529,700; and 3) Single Sign On capability - $170,500.

The purpose of the proposed upgrades is to provide operational infrastructure that restores critical business services in the event of a localized disaster to the PERS main data center in Tigard. The project is driven by a need for PERS to improve its disaster recovery and business continuity processing capabilities to assure compliance with the requirements of the current Department of Administrative Services (DAS) Statewide Business Continuity Planning Policy (107-001-010). This policy directs agencies to establish specific performance and availability requirements related to the system performance and the number of business days per month that mission critical agency information systems, like the Oregon Retirement Information On-line Network (ORION), are not available. DAS, now the State Chief Information Officer, also has information security related policies (i.e. Information Security Policy - 107-004-052) in place that direct agencies to ensure that agency IT infrastructure meets specific security requirements. Together these disaster recovery, business continuity, and information security policies provide clear direction to agencies on what actions they must take to protect state IT resources.

The four major high-level objectives for this initiative include the establishment of:

1. The "disaster recovery infrastructure" required to overcome a localized event that compromises PERS's hosted systems.
2. A "virtual desktop environment" to reduce current hardware requirements and facilitate remote operations when required.
3. A "single sign-on" (SSO) protocol.
4. An updated and tested "business continuity plan" (utilizing the new tools).

The proposed upgrade of PERS's existing disaster recovery infrastructure will also help assure that monthly benefit payments of over $350 million would continue to be provided should PERS's hosted

information systems be disrupted.  The proposed upgrade also provides PERS with a virtual desktop capability for allowing remote access and business continuity capabilities should the primary PERS data center or service center in Tigard become unavailable.  In addition, the initiative provides seamless and secure access between PERS application systems via the SSO capability.  The initiative was originally scheduled to begin on July 1, 2015 and end on July 1, 2017 but was delayed per legislative direction given to the agency during the 2015 legislative session.

For the 2015-17 budget, $1,581,200 in Other Funds expenditure limitation was approved, but unscheduled, to allow PERS to complete a detailed health check and risk assessment of the current state of PERS's disaster recovery and business continuity environment, including the state of its current related DR and BCP plans.  In addition, PERS was requested to develop a detailed action plan(s) for implementing robust disaster recovery and business continuity planning programs.

**A.  LFO Analysis**

The Legislative Fiscal Office (LFO) review of POP #105 (2015) budget-related materials provided by PERS during the 2015 legislative session clearly identified that PERS had a number of risks related to its disaster recovery and business continuity planning efforts.  However, it was not clear what the actual state of PERS's DR and BCP programs were, how significant were the risks that PERS was facing, nor was it clear how many of the outstanding disaster recovery and business continuity risks would actually be addressed by the proposed policy option package.  As such, during the 2015 legislative session, PERS was requested to complete the following key actions prior to any of the $1,581,200 approved expenditure limitation being rescheduled:

1. Immediately increase the offsite storage frequency of PERS "disaster recovery tapes," from once weekly to daily, to immediately mitigate this obvious and unnecessary risk.
2. Conduct a detailed risk assessment of the current state of PERS's disaster recovery and business continuity environment (including the status of the current "disaster recovery and business continuity plans").  Include a detailed priority analysis and list of the key DR/BCP-related problems and risk areas that are identified within the assessment.  Develop an action plan based upon this risk assessment.  Review the findings of this assessment with both the Office of the State Chief Information Officer (OSCIO) and LFO.
3. Provide both the OSCIO and LFO with an analysis of the PERS 2015-17 information technology workload, clearly showing how this project can be timely completed, given the magnitude of what is already on PERS's "platter" for the 2015-17 biennium.
4. Provide both the OSCIO and LFO with a prioritized go-forward plan (including the justification for each priority) that would allow the more critical elements of this project to be the focus of initial PERS efforts, with less critical elements being delayed later in the 2015-17 biennium.
5. Early in the project, work with the OSCIO and LFO to determine which elements of the Joint State CIO/LFO Stage Gate Review Process will be followed for a project of this type, including what key deliverables will be required.
6. Work with OSCIO and LFO to finalize a corresponding incremental funding release plan that is based upon a prioritized implementation plan for each of the prioritized three key components of POP #105.
7. Work closely with and regularly report project status to the OSCIO and LFO throughout all elements of the project's lifecycle.
8. Utilize a qualified project manager with experience in planning and managing programs and projects of this type, scope, and magnitude.

9.  Develop appropriate foundational project management documents, and provide all key documents to the QA vendor for quality reviews.
10. Work with OSCIO to obtain independent quality management services.  The contractor shall:
    a.  Conduct an initial risk assessment.
    b.  Perform quality control reviews on the key project deliverables including the business case, individual cost benefit/alternatives analysis documents, and foundational project management documents as appropriate.
    c.  Perform ongoing, independent quality management services as directed by the OSCIO.
    d.  Submit all key project documents, the initial risk assessment, and quality control reviews to the OSCIO and LFO.
11. Regularly report to the OSCIO and LFO on project progress and on the development of key project documentation.
12. Utilize the OSCIO's Enterprise Project and Portfolio Management (PPM) system as it is deployed for all project review, approval, and project status and QA reporting activities throughout the life of the project.

LFO met with PERS disaster recovery and business continuity program staff periodically throughout the 2015 interim, and PERS provided some high-level work products related to implementing more robust programs for both disaster recovery and business continuity.  However, a majority of the twelve action items identified above were not adequately addressed by PERS.  In particular, items #2 and #4 were not addressed sufficiently, although PERS did provide a basic overview plan of how it proposed to implement more robust disaster recovery and business continuity programs.  However this "plan" was not based upon a solid detailed risk assessment of the current state of PERS's disaster recovery and business continuity environment (including the status of the current disaster recovery and business continuity plans).  In addition, PERS did not include a detailed priority analysis and list of key DR/BCP related problems and risk areas that were supposed to be identified within the assessment.  Nor did PERS develop a detailed action plan based upon this risk assessment and review the findings of this assessment with both the OSCIO and LFO.  The bottom-line is that PERS did not specifically respond in detail to each of the twelve instructions provided in the recommendations adopted by the 2015 Information Technology Subcommittee of the Joint Committee on Ways and Means.

PERS did provide LFO with some high-level materials related to POP #105 and the twelve legislative instructions identified above (in particular items #2 and #4).  However, as noted above, the materials submitted in mid-January 2016 were not adequate to meet the twelve legislative requirements of the legislative direction provided for POP #105.  The materials that were provided to LFO included:

*   A Request/Report Letter (January 22, 2016) to Joint Committee on Ways and Means leadership on its progress on legislative instructions for POP #105 (2015).  This letter only provided only minimal "progress" and status report information on PERS progress on legislative instructions for POP #105.
*   A high-level status matrix on progress on the twelve legislative instructions.
*   A four-page high-level response to POP #105 legislative instructions #2 and #4.
*   A high-level project charter for POP #105 - Disaster Recovery Infrastructure Upgrades.

In addition to these concerns regarding PERS progress on legislative instructions related to PERS POP #105 (2015), LFO, in consultation with the Office of the State Chief Information Officer (OSCIO), was made aware that PERS had not responded to previous legislative requests and commitments to the

DAS/OSCIO to clearly define the rationale and need for PERS to maintain its own data center and related infrastructure when the Retirement Information Management System (RIMS) Conversion Program was completed several years ago. The OSCIO, via the Enterprise Technology Services (ETS) state data center, currently provides data center services similar to those provided by PERS's internal data/service center, has brokered cloud services contracts in place, and also has highly robust disaster recovery and business continuity services available for agency use.

On a final related issue, PERS POP #105 (2015) proposes the acquisition of mainframe, server, network hardware, and related software that must be reviewed and approved by the OSCIO. State agencies are prohibited from acquiring these types of hardware assets regardless of dollar amount without the review and approval of the OSCIO per the State IT Investment Review and Approval Policy (107-004-130). Prior OSCIO approval must be acquired before the acquisition of any hardware or software assets being proposed for purchase by PERS.

## B. LFO Recommendations

Based upon LFO's review of the materials submitted by PERS related to the legislative direction provided to PERS during the 2015 legislative session on POP #105 (2015), LFO recommends that the entire expenditure limitation that was unscheduled during the 2015 legislative session remain unscheduled. In addition, LFO recommends that PERS:

- Conduct a joint data/service center analysis and assessment with the OSCIO, of the justification for PERS maintaining and operating its own data/service center in Tigard.
- Refrain from the acquisition of any mainframe, mid-tier, hardware/software infrastructure without prior review and approval of the OSCIO per statewide policy (107-004-130).
- Provide OSCIO with copies of all disaster recovery and business continuity related plans, policies, standards, guidelines, programs, and related documentation for review.
- Conduct a joint detailed independent risk assessment with the OSCIO of the current state of PERS's disaster recovery and business continuity environment (including the status of the current "disaster recovery and business continuity plans"). Include a detailed priority analysis and list of the key DR/BCP-related problems and risk areas that are identified within the assessment. Develop an action plan based upon this risk assessment. Review the findings of this assessment with both the OSCIO and LFO.
- Report the findings and recommendations of the joint data center analysis and assessment to the Legislature during the December 2016 Legislative Days.
- Report the findings and recommendations of the joint detailed risk and security assessment of the current state of PERS's disaster recovery and business continuity environment to the Legislature during the December 2016 Legislative Days.

  - Motion on the LFO recommendations

## C. Final IT Subcommittee Action

Transmit the JLCIMT recommendations to the General Government Subcommittee of the Joint Committee on Ways and Means.