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:	November 14, 2017
Subject:	Public Employees Retirement System: Progress Report on Budget Notes for SB 5534 (2017) - Budget Notes #1, #3, and #4 - LFO Analysis and Recommendations

Agency Request:
The 2017 Legislature directed the Public Employees Retirement System (PERS), under the direction of the Department of Administrative Service (DAS) - Office of the State Chief Information Officer (OSCIO), to jointly report the status and progress on four budget notes related to SB 5534 (2017). These budget notes focused on: 1) developing a robust certified cybersecurity program (including completely responding to the Joint OSCIO/LFO Security Memo – April 7, 2016) on PERS security deficiencies; 2) the Individual Account Program (IAP); 3) the feasibility analysis and related development of a migration plan, schedule, and budget for migrating PERS to the State Data Center (SDC)/Enterprise Technology Services (ESO); and 4) the development and certification of a business continuity program, a disaster recovery program, and the acquisition of an appropriate disaster recovery warm-site.

PERS and OSCIO were directed to report the progress on each of these budget notes to the Interim Joint Legislative Committee on Information Management and Technology (JLCIMT) during the legislative days in September and November, and during the 2018 Legislative session. The Public Employees Retirement System has submitted its progress report to the JLCIMT on the progress of the four budget notes. LFO has submitted a separate analysis on budget note #2, the Individual Account Program (IAP). This second LFO analysis focuses on budget notes #1, #3, and #4.

The agency requests acknowledgement of receipt of its report on the three remaining SB 5534 (2017) budget notes (Budget Note #1 – Cybersecurity Program, Budget Note #3 – State Data Center Migration, and Budget Note #4 – Business Continuity Program, Disaster Recovery Program, and Warm-Site Acquisition).

A. LFO Analysis

Background

During the 2017 legislative session, PERS submitted several funding requests related to modernizing its application system environment, correcting technical debt issues, establishing a cybersecurity program, enhancing business continuity and disaster planning capabilities, and implementing a warm-

site capability. An LFO review of these requests indicated that they would not in a timely manner, sufficiently address long-standing PERS deficiencies in security, business continuity, and disaster planning. Based upon LFO's assessment that PERS: 1) had still not made sufficient progress in addressing its long-standing security deficiencies identified in the Joint OSCIO/LFO Memorandum on PERS security – April 7, 2016; 2) had not completed the required data center feasibility study requested by the JLCIMT in February 2016; and 3) had not provided a solid plan for addressing deficiencies in its business continuity and disaster recovery capabilities, LFO recommended that a majority of PERS's IT-related budget requests not be approved. Instead, LFO recommended the following:

1. Deferment of all PERS requested funding for technical debit and modernization.
2. The establishment of 3.0 FTE's to develop and support PERS's cybersecurity program. These positions were to be transferred to the Enterprise Security Office (ESO) of the OSCIO.
3. Funding in the amount of $250,000 for developing a PERS business continuity program.
4. Funding in the amount of $500,000 for developing a PERS disaster planning program.
5. Funding in the amount of $1,147,634 for acquiring a PERS disaster recovery warm-site.

LFO also recommended a set of four budget notes for SB 5534 (2017) to help make sure that PERS and OSCIO made significant timely progress on dealing with the PERS deficiencies. The Legislature, through these four separate budget notes for SB 5534, directed PERS to focus first on its long-standing issues related to its security, business continuity, and disaster planning environment and capabilities, before returning its focus to technical debt and modernization needs for its existing technical infrastructure and application system environment.

Three of the budget notes focused primarily on technical related deficiencies (security, data center migration, disaster recovery, business continuity, and warm-site acquisition). The fourth budget note focused on PERS's IAP Project, which was struggling with major scope issues and the loss of its key development contractor. PERS and OSCIO were directed to report progress on these four budget notes to the JLCIMT during the September and November 2017 legislative days, and also to the 2018 legislative session. Through these four budget notes for SB 5534 (2017), the Legislature hoped to have PERS and OSCIO achieve the following goals by the end of the 2017-19 biennium:

1. Successful insourcing of the IAP into PERS for administration and operation.
2. Joint OSCIO/LFO Security Memo (April 7, 2016) recommendations fully addressed.
3. PERS Security Program (industry standard) fully implemented, tested, and certified.
4. PERS Business Continuity Program (industry standard) fully implemented, tested, and certified.
5. PERS Disaster Recovery Program (industry standard) fully implemented, tested, and certified.
6. Completion of the State Data Center (SDC)/Enterprise Technology Services (ETS) power upgrade to allow PERS to migrate its in-house Tigard-based data center to the SDC/ETS.
7. PERS data center fully migrated to SDC/ETS (current PERS data center de-commissioned).
8. Development, implementation, and testing of a PERS "warm-site" capability (part of PERS's disaster recovery effort).

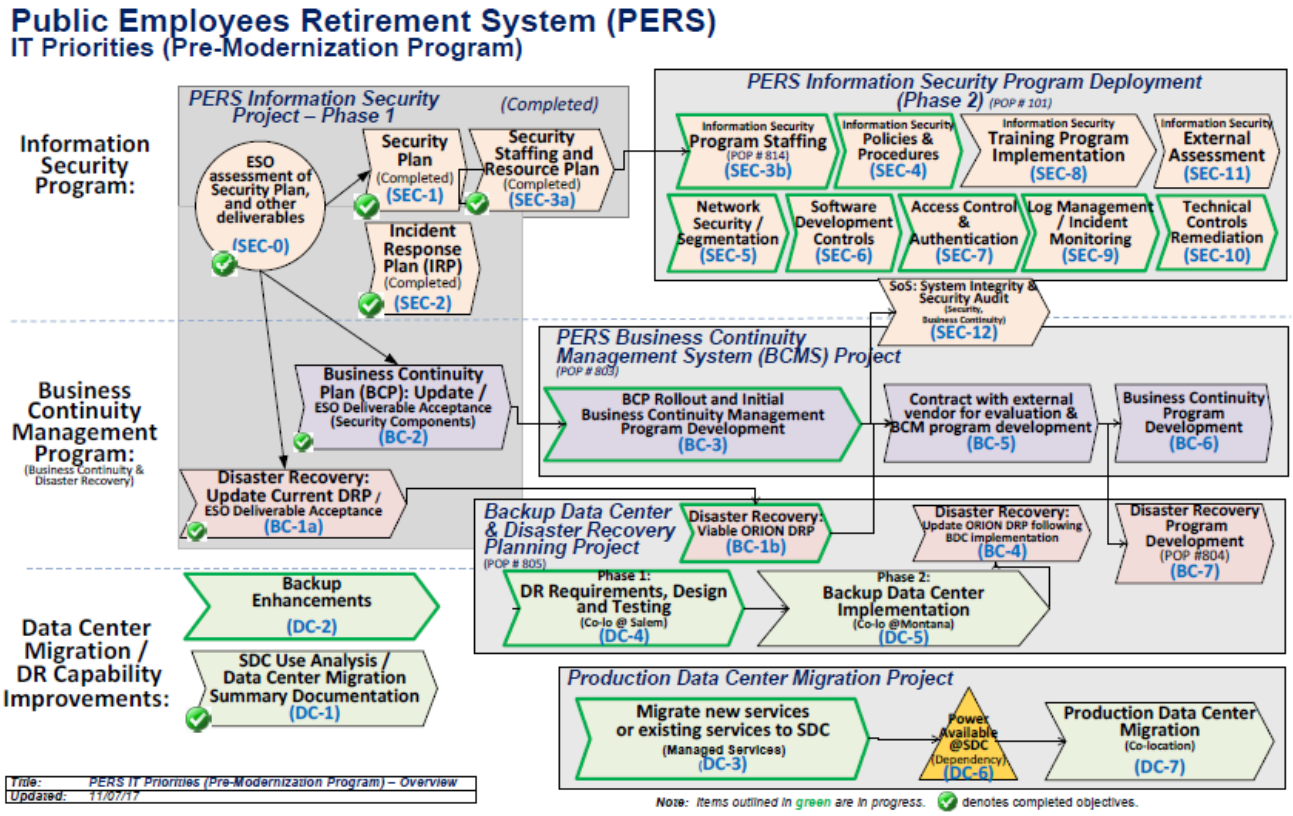
9. The changing of PERS's backup medium from tapes to an ETS standard compatible medium (part of business continuity and disaster recovery efforts).
10. Development and implementation of both short-term and ongoing PERS business continuity and disaster recovery capabilities to mitigate current risks until the industry-standard Business Continuity Program and the Disaster Recovery Program are tested and in place.
11. Development and implementation of both short-term and ongoing PERS security operational support while a PERS's industry-standard cybersecurity program is developed and implemented by the Enterprise Security Office (ESO).
12. Development and updating of the PERS's Business System Plan (BSP), Information System Plan (ISP), Enterprise Architecture Plan (EAP), and Modernization Plan, to help assure that PERS is ready to move forward with its modernization of the ORION/jClarety technical and application systems environments (once the three technically-focused budgets notes are completed).

The Legislature expected PERS to forego any additional system and technical debt enhancements and modernization of its ORION and jClarety systems until all of these goals were achieved. This specific direction was given due to the seriousness of the deficiencies that were identified in PERS's security, disaster recovery, and business continuity capabilities, and the resulting risks to PERS's ability to continue to conduct business in the event of localized or regional disasters.

A summary of LFO's assessment of PERS's and OSCIO's progress on each of the three technical budget notes, the individual projects that are being established to address each of the three budget notes, and the twelve specific goals identified above follows.

LFO Findings

From July through September of 2017, LFO met with OSCIO management staff to identify approaches and strategies for dealing with the three technical budget notes related to PERS security, business continuity, disaster recovery, data center migration, and warm-site acquisition. It was agreed that individual projects would be set up for each major initiative, that these projects would be run with Project Management Body of Knowledge (PMBOK) discipline, and that the work related to responding to the Legislative budget notes for SB 5534 (2017) would be done by PERS, OSCIO, and external contracted staff. LFO's role was to provide legislative expectations and goals, basic rules of engagement for how the work would get done and how status would be reported, and technical oversight of all projects and initiatives. OSCIO coordinated with PERS management and technical staff on the basic rules of engagement, the proposed go-forward strategies, and general LFO expectations. As part of this process, the OSCIO leadership proceeded to work with PERS and the Enterprise Security Office (ESO) to develop the go-forward strategies chart provided below. This chart attempts to show all the major components of the work that needs to be done to fully respond to the three technical budget notes that are the focus of this analysis.



While this chart does not at this time provide detailed schedules and dates for when all of the work will be completed, its development was essential in determining how many projects would need to be set up and managed. The planning work required to develop this chart resulted in the identification of the following projects and related initiatives which are critical to fully responding to the legislative budget notes for SB 5534 (2017):

1. PERS Information Security Program Planning (completed - part of Budget Note #1);
2. Joint LFO/OSCIO Security Memorandum - April 7, 2016 - (Budget Note #1);
3. PERS Cybersecurity Program Project - (Budget Note #1);
4. State Data Center (SDC) Migration Project - (Budget Note #3);
5. Business Continuity Program Project (Budget Note #4);
6. Disaster Recovery Program Project (Budget Note #4); and
7. Warm-Site Acquisition Project (Budget Note #4).

Joint LFO/OSCIO Security Memorandum -April 7, 2016
(Budget Note #1)

In 2015, PERS initiated an independent assessment of its security environment. The resulting 2016 "IT Security Program Review" report identified information security deficiencies related to PERS's behavioral, procedural, and technical practices. LFO was briefed by OSCIO on the high-level findings of this independent external assessment. Simultaneously, the Governor's Office directed PERS to work with OSCIO and LFO to make sure that these deficiencies were dealt with in a timely manner. On April 7, 2016, a joint memorandum was produced by OSCIO and LFO. This memorandum, entitled

"Joint OSCIO/LFO Memorandum" provided PERS with specific directions, including sixteen recommendations for dealing with the key findings of PERS's security assessment. The expectation was that PERS would deal with these sixteen recommendations by June 30, 2017.

During 2016, PERS worked with OSCIO to address the 16 specific areas of security-related deficiencies that needed to be addressed. To help get this work done, PERS hired an external vendor. This vendor was asked to help assess PERS capabilities, deficiencies, and maturity in its security, business continuity, and disaster recovery business processes and capabilities. Unfortunately, only a limited amount of their work was directed towards actually helping remediate security deficiencies. Much of their work focused more on assessment than remediation. On May 26, 2017, PERS and the external vendor conducted a contract close-out meeting for PERS, OSCIO, and LFO. At this meeting, the vendor's findings and PERS's progress to date on the sixteen recommendations were reported. The vendor reported that they had completed the requirements of their contract with PERS, provided a summary of their findings, and PERS reported on their progress to date on the sixteen recommendations.

PERS reported that they had made significant progress on the sixteen recommendations, however, after OSCIO and LFO completed their reviews of actual progress, it appeared that only three of the total sixteen recommendations were fully addressed and completed (though there was additional progress on the remaining thirteen outstanding recommendations). OSCIO and LFO both informed PERS of their concerns related to the limited progress on the sixteen recommendations, after nearly a year's time (April 2016 through May 2017).

In September 2017, OSCIO and the Enterprise Security Office (ESO) completed its formal review of PERS progress on the sixteen security related recommendations that came out of the Joint OSCIO/LFO Memorandum - April 7, 2016. This review showed five of the sixteen recommendations completed, with eleven others "in-progress." While not all of the sixteen recommendations were of the same size and importance, both OSCIO and LFO felt that this was insufficient progress for nearly 15 months of effort. In particular, LFO was concerned with the fact that there had been only limited progress on recommendation #2 - Formalize PERS Information Security Program and improve internal communication. While some progress has been made on this effort, LFO was concerned that a robust, industry standard security program was still not in place within PERS. A more detailed discussion of this specific recommendation and related LFO concerns follows in the next section

Cybersecurity Program
(Budget Note #1)

The Joint OSCIO/LFO Memorandum (dated April 7, 2016) on PERS security deficiencies, specifically identified the need for PERS to take aggressive steps to define, develop, implement, and test a robust internal Security Program (not just a "security plan"). As mentioned in the previous section, the OSCIO review of PERS progress on the sixteen security recommendations (September 2017), clearly showed that this key goal had not yet been completed by PERS. In fairness, implementing a major security program is not an overnight task, and requires a significant number of highly trained security resources (which PERS does not currently have).

To help expedite the development of this program, LFO worked with PERS and the ESO to identify additional PERS security resource needs that could be acquired and utilized to expedite the security program's definition and implementation. During the 2017 Legislative Session, an additional 3.0 FTE's were provided to PERS to help beef up its security staff. In turn, these positions were re-directed to the ESO so that they could be focused solely on defining, developing, and implementing PERS's Security Program (recommendation #2 of the Joint OSCIO/LFO Memorandum). These staff have been hired and are currently working within the ESO to help PERS develop its cybersecurity program.

As part of setting up the PERS Security Program, the ESO has recently reviewed and approved PERS's current Security Plan, its Security Staffing and Resource Plan, and Incident Response Plan. The ESO has provided LFO with an initial project charter, and the ESO has been providing LFO with regular status reports on this project team's efforts to date. At this time, the final implementation date for the PERS Cybersecurity Program is not clearly defined, though LFO has been told that the ESO plans on having the PERS Cybersecurity Program fully implemented by the end of 2018.

LFO has asked OSCIO to develop a detailed workplan, including a project schedule, budget, and resource plan, to help with the tracking of the development, implementation, and certification of the newly developed PERS cybersecurity program. Overall, LFO is satisfied with the initial progress on the PERS cybersecurity program. Properly trained security resources are in place to get PERS's cybersecurity program developed and implemented, and the ESO has assured LFO that the necessary Project Management Body of Knowledge (PMBOK) artifacts needed to properly manage and track this effort will be completed in the near future.

State Data Center Migration
(Budget Note #3)

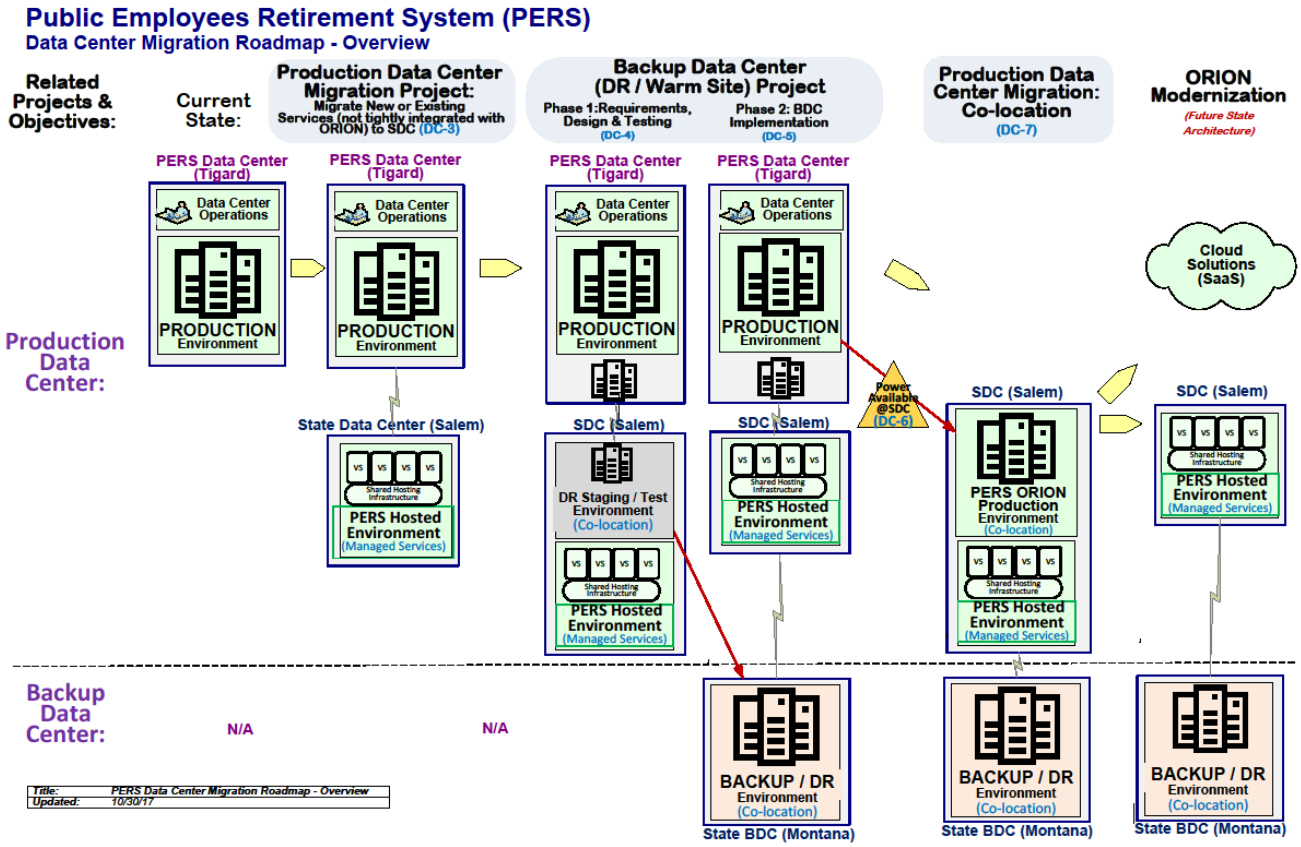
In the 2015-17 (2016) legislative session, PERS was directed to develop a feasibility study to analyze why PERS needed to have its own internal, on-site data center. Several years before, previous PERS leadership had committed to the Legislature that it would be migrating its Tigard-based data center to the State Data Center (SDC) in Salem. As such, in 2016, the JLCIMT requested PERS to analyze why it shouldn't take advantage of the robust SDC, and not only reduce costs, but be able to take advantage of SDC's strong security, disaster recovery, and business continuity capabilities. PERS did not fully respond to the legislative instructions from the 2016 legislative session until just recently. In early November 2017, the OSCIO and PERS provided LFO with a copy of their analysis entitled, State Data Center (SDC) Use Analysis and Data Center Migration Summary (November 1, 2017).

While the provided document was not the actual feasibility study and robust options analysis that was requested by the Legislature, it did provide a roadmap. It also provided the results of work between PERS, OSCIO, and the ESO that clearly showed that there was general agreement between the parties and that there was sufficient business, technical, and financial justification for PERS to migrate its data center services to the SDC. Once this migration was complete, PERS could then decommission the current PERS internal Tigard-based data center.

The PERS document also showed that it was clear to all parties involved that this effort had key dependencies on several other projects and initiatives, including the SDC upgrading its facility's power, coordination with the PERS warm-site acquisition effort, and coordination with the PERS business continuity and disaster recovery efforts (both short-term and long-term).

Since the 2017 legislative session, a strategy (including co-location and managed service approaches) to migrate the PERS data center has been developed, a basic project charter has been developed, and PERS has begun the development of critical project planning documentation. Currently, there is no firm timeline, list of milestones, project budget, resource plan, or status reporting plan in place to help PERS, OSCIO, and LFO track progress on this effort. PERS and OSCIO have indicated that these important project management artifacts will be developed in the near future.

The roadmap diagram below provides an overview of the detailed planning that has been undertaken for the migration of the PERS Tigard-based data center to the SDC/ETS data center.



Overall, LFO is satisfied with the initial planning efforts for migrating PERS's data center to the SDC. That said, it is important that this effort be formalized into a well-defined project and that PERS implement regular project status reporting, such that oversight (both OSCIO and LFO) can properly track the effort.

Business Continuity Program
(Budget Note #4)

Budget Note #4 for SB 5534 (2017) requires PERS to develop and implement a robust, industry-standard business continuity program (not just a plan), and to have this program assessed and certified. In order to avoid disruptions in services (i.e. loss of power, equipment failure, loss of all or part of PERS's network, loss of a server, etc.) and be able to assure the continuation of its business services, PERS needs to have a robust business continuity program in place. This program needs to be closely integrated with PERS's disaster recovery program, and security program.

PERS has made the following progress on its business continuity program (and related disaster recovery program efforts): 1) developed a draft project charter; 2) developed a draft business continuity plan and provided this plan to OSCIO; 3) had the "security" components of PERS's business continuity plan reviewed by ESO; and 4) established a plan for reviewing, approving, testing, and training on this draft business continuity plan. Overall, LFO is satisfied with the initial planning efforts for setting up a project that will result in the development of an industry-standard business continuity program. However, it is important that these initial efforts be formalized into a well-defined project, and that PERS implement regular project status reporting, such that oversight (both OSCIO and LFO) can properly track the effort. In addition, due to the lack of sufficient available business continuity trained staff within both PERS and OSCIO, PERS needs to immediately acquire highly trained external consulting support to facilitate the development of its business continuity program.

PERS has recently notified both OSCIO and LFO that it has been contacted by the Secretary of State (SOS) Audits Division, regarding an upcoming external assessment that will look at a wide-range of PERS functions and capabilities, including system integrity, security, and business continuity.

Disaster Recovery Program
(Budget Note #4)

Budget Note #4 for SB 5534 (2017) requires PERS to develop and implement a robust, industry-standard disaster recovery program (not just a plan), and to have this program assessed and certified. In order to recover its business functions in the event of a major disaster (i.e. loss of the Tigard business center or the loss of the co-located PERS data center), PERS needs to have a robust disaster recovery program in place. This program needs to be closely integrated with PERS's business continuity program, and security program.

PERS has made the following progress on its disaster recovery program (and related warm-site effort): 1) developed a draft project charter; 2) developed a draft disaster recovery plan and provided this plan to OSCIO; 3) acquired an external consultant for planning and testing for Phase 1 of the disaster recovery and warm-site effort; and 4) identified an enterprise data backup solution to replace its current backup infrastructure.

Overall, LFO is satisfied with PERS's and OSCIO's initial planning efforts for setting up a project that will result in the development of an industry-standard disaster recovery program. However, it is important that these initial efforts be formalized into a well-defined project, and that PERS

implement regular project status reporting, such that oversight (both OSCIO and LFO) can properly track the effort. In addition, due to the lack of sufficient available disaster recovery trained staff within both PERS and OSCIO, PERS needs to immediately acquire external highly trained consulting support to facilitate the development of its disaster recovery program.

Warm-Site Acquisition
(Budget Note #4)

As part of PERS's overall business continuity and disaster recovery efforts, PERS needs to have a warm-site capability to allow PERS to continue to do business should a disaster result in the existing Tigard data center no longer being able to provide needed data center services. The same warm-site capability will be required once PERS migrates its data center to the SDC/ETS. In 2017, the Legislature provided PERS with $1,147,634 in funding to define, develop, and implement this capability.

Since the 2017 legislative session, PERS and OSCIO have worked on developing a set of strategies and a plan for acquiring a warm-site for PERS. As mentioned earlier, there are interdependencies between many of the projects and initiatives that have been identified, and PERS must consider these interdependencies to assure that it is fully responding to the budget notes for SB 5534 (2017).

PERS has made the following progress on its warm-site effort: 1) initial project planning including the development of a project charter; 2) acquisition of an external consultant for planning and testing for Phase 1 of the project; and 3) identification of an enterprise data backup solution to replace its current backup infrastructure. Overall, LFO is satisfied with the initial planning efforts for the acquisition of a PERS warm-site capability. However, it is important that this effort be formalized into a well-defined project and that PERS implement regular project status reporting, such that oversight (both OSCIO and LFO) can properly track the effort.

Findings Summary

A summary of LFO's major findings on PERS's and OSCIO's recent efforts and progress related to the three technical-related budget notes (#1, #3, and #4) for SB 5534 (2017) follow:

1. Overall, PERS, OSCIO, and the ESO have made good progress on the initial planning for setting up projects to address each of the three budget notes. However, there is still a significant amount of remaining project management setup work to be done before actual work can be initiated on a majority of these projects.
2. PERS and OSCIO need to focus on further developing the PMBOK and OSCIO/LFO Stage Gate Review Process related project management artifacts (i.e. charters, project management plans, workplans, schedules, budgets, resource plans, risk logs, status reports, etc.) to allow each of these efforts to be managed and overseen effectively.

3. PERS, OSCIO, and ESO have recently focused a lot of needed attention on making sure that PERS's ability to immediately respond effectively to incidents, events, and localized and regional disasters are timely and effective. These procedures are critical for PERS to be able to assure the continuity of its business services now, while the more robust business continuity and disaster programs are being developed and implemented.
4. Neither PERS or OSCIO currently have sufficient available highly-trained business continuity and disaster recovery staff to support the timely development and implementation of the needed programs. Every effort should be made to acquire these needed technical resources through external vendor organizations. In addition, OSCIO should assess the state's needs for acquiring permanent state staff within OSCIO and ETS to provide long-term support for enterprise-wide business continuity and disaster planning needs.
5. Status reporting to date on the three technical budget notes and the related 5-6 projects that are in the process of being set-up, has been inadequate. The single page overall status report that was provided to OSCIO and LFO by PERS at the first of November, was not adequate to provide effective oversight and tracking of progress on the 5-6 major highly interrelated projects. While LFO realizes that a majority of these projects are not fully set up as yet, significant improvements still need to be made in the status reporting and communications between all parties involved in these efforts.

B. LFO Recommendations

Based upon the analysis and findings above, LFO recommends:

1. Acknowledging receipt of the progress report for the technical budget notes #1, #3, and #4 for SB 5534 (2017).
2. Directing PERS to report progress at the January 2018 JLCIMT on the cybersecurity program, the Joint LFO/OSCIO Memorandum – April 7, 2016 on PERS security, the SDC data center migration effort, the definition and implementation of a business continuity program, the definition and implementation of a disaster recovery program, and the acquisition of a "warm-site" capability.
3. Directing PERS and OSCIO to respond to LFO findings and concerns identified above, and to provide evidence to the JLCIMT at the January 2018 JLCIMT hearing, that steps have been taken to make sure that these concerns are addressed.
4. Directing PERS and OSCIO to come to the JLCIMT during the 2018 legislative session with a stakeholder approved detailed schedule, milestones and deliverables list, budget, and resource plan for each of the projects that support the three technical budget notes for SB 5534 (2017).
5. Directing PERS and OSCIO to come to the JLCIMT during the 2018 legislative session and provide a plan for leveraging external business continuity and disaster planning vendors to assure adequate highly trained technical resources and expertise is available to support these efforts.

C. Recommended JLCIMT Action

Acknowledge receipt of the report, with instructions.
Note: LFO will share the JLCIMT analysis and instructions with members of the General Government Subcommittee of the Interim Joint Committee on Ways and Means.