Report of the Joint Committee on Information Technology to the 2015 Kansas Legislature

CHAIRPERSON: Senator Mike Petersen

VICE-CHAIRPERSON: Representative Keith Esau

OTHER MEMBERS: Senators Marci Francisco, Tom Holland, Garrett Love, and Jeff Melcher; and Representatives Steven Johnson, Kevin Jones, Harold Lane, and Brandon Whipple

CHARGE

- Study computers, telecommunications, and other information technologies used by state agencies and institutions;
- Review proposed new acquisitions, including implementation plans, project budget estimates, and three-year strategic information technology plans of state agencies and institutions;
- Monitor newly implemented technologies of state agencies and institutions;
- Make recommendations to the Senate Committee on Ways and Means and the House Committee on Appropriations on implementation plans, budget estimates, and three-year plans of state agencies and institutions; and
- Report to the Legislative Coordinating Council and make special reports to other legislative committees, as deemed appropriate.

Joint Committee on Information Technology

Report

Conclusions and Recommendations

The Committee recommends the executive branch Chief Information Technology Officer (CITO) develop an enterprise-level information technology security plan to determine which security functions should be centralized and which security functions should be performed by individual agencies. In addition, the CITO should bring back recommendations to the Committee regarding which security functions should be performed by state agencies, and which functions should be outsourced to the private sector.

The Committee further recommends consideration of incorporating a return-on-investment component for proposed large information technology projects. Each proposal for an information technology project should include a return-on-investment section, following a life-cycle methodology, and include all follow-up information documenting savings or efficiencies as part of project plans; that documentation should be maintained throughout changes and developments within each project's life-cycle.

The Committee recommends each respective branch CITO identify security vulnerabilities regarding sensitive information and propose remediation actions. In addition, the Committee recommends the branch CITOs identify critical systems lacking continuity of operations plans which would be utilized for disaster recovery purposes.

The Committee recognizes and commends the Legislative CITO on the progress made on legislative information technology projects, in particular, the Kansas Legislative Information Systems and Services (KLISS) project, and his diligence in keeping the Committee apprised of the progress in development, phases, and implementation.

Proposed Legislation: None.

Background

The Joint Committee has statutory duties assigned by its authorizing legislation in KSA 46-2102 as noted below, and the three statutory duties also defined its general areas of interim activity:

- Study computers, telecommunications, and other information technologies used by state agencies and institutions. The state governmental entities defined by KSA 75-7201 include executive, judicial, and legislative agencies and Regents institutions;
- Review proposed new acquisitions, including implementation plans, project budget estimates, and three-year strategic information technology plans of state agencies and institutions. All state governmental entities are required to comply with provisions of KSA 75-7209 *et seq.* in submitting such information for review by the Joint Committee; and
- Monitor newly implemented technologies of state agencies and institutions.

The Joint Committee on Information Technology (JCIT) met during the 2014 Interim, as authorized by the Legislative Coordinating Council.

The Committee heard reports from the Chief Information Technology Officers (CITOs) for the executive, judicial and legislative branches of government, a special audit on security issues was also presented by the Legislative Division of Post Audit staff, and specific project updates were heard on the executive branch enterprise email system, and the judicial branch electronic filing system.

The Committee had received a presentation regarding the executive branch enterprise email system at its April 2, 2014, meeting, in which it had also received reports that the system might present security and compatibility concerns for public safety agencies. The most recent report received at the November 13, 2014, meeting noted that this issue was being addressed, and that the system would be compatible with those public safety agencies and for those systems that had initially expressed concerns.

In continued review of information security the Committee held an executive session meeting on May 1, 2014. A Novacoast executive was available at that meeting in order to answer questions and lead discussion regarding IT security. These ideas were further explored at the November 13th meeting where Legislative Post Audit staff presented its report on: 'State Agency Information Systems: Sensitive Datasets and IT Security Resources' (July 2014, R-14-007).

Conclusions and Recommendations

The Committee recommends the Executive branch CITO develop an enterprise-level information technology security plan to determine which security functions should be centralized and which security functions should be performed by individual agencies. In addition, the CITO should bring back recommendations to the Committee regarding which security functions should be performed by state agencies, and which functions should be outsourced to the private sector.

The Committee further recommends consideration of incorporating a return-on-investment component for proposed large information technology projects. Each proposal for an information technology project should include a return-on-investment section, following a life-cycle methodology, and include all follow-up information documenting savings or efficiencies as part of project plans; that documentation should be maintained throughout changes and developments within each project's life-cycle.

The Committee recommends each respective branch CITO identify security vulnerabilities regarding sensitive information and propose remediation actions. In addition, the Committee recommends the branch CITOs identify critical systems lacking continuity of operations plans which would be utilized for disaster recovery purposes.

The Committee recognizes and commends the Legislative CITO on the progress made on legislative information technology projects, in particular the Kansas Legislative Information Systems and Services (KLISS) project, and his diligence in keeping the Committee apprised of the progress in development, phases, and implementation.