Testimony regarding Senate Bill 2 - Information Technology Audits

To the House Appropriations Committee

March 20, 2013

Presented by Anthony Schlinsog, Executive Branch Chief Information Technology Officer Governor's Office of Information Technology Services

Mr. Chairman and members of the committee, my name is Anthony Schlinsog, and I am the Chief Information Technology Officer for the Executive Branch. Thank you for the opportunity to appear before your committee today to share my thoughts on an alternative approach to accomplishing the goals of a specific provision of Senate Bill 2 regarding the institution of continuous audits of ongoing IT projects by the Division of Legislative Post Audit.

Since its passage in 1998, K.S.A. 75-7205 has defined the role of Executive Chief Information Technology Officer in oversight of information technology projects in the Executive Branch. This responsibility is executed within an IT governance framework that involves the participation of my counterparts in the Judicial and Legislative Branches who perform similar roles for the IT projects in their respective branches. Another statute, K.S.A. 75-7209, outlines the procedures to be used in approval and oversight of these projects.

This oversight begins in the earliest phases of the project, starting with its identification in the agency's three-year IT management and budget plan that is submitted annually to the Legislature, and proceeding through required approvals by me along with the agency head for the cost-benefit analysis for the project, the bid specifications and requirements for procurements associated with it, and detailed plans for the project. As the project proceeds, we require ongoing reporting against the plan, and report progress and status every 90 days to the Legislature.

This governance structure has been very effective. In a review undertaken at the end of 2011, over 163 projects had been delivered successfully since 2004, with only 4 projects cancelled, with an average final cost coming within 10% or less of the original approved cost. In a companion effort, the state's IT workforce is trained and certified in the management of IT projects. To-date, almost 400 state IT project managers have completed this certification, along with other training meant to improve the skills of our project management workforce in risk assessment, business case preparation and similar topics. Finally, state project managers have worked with their teams to prepare over 140 post-implementation evaluation reports (PIER) that assess the work done during their project, as well as document lessons learned and recommendations for improvement in future projects.

Troubled or even failed projects are of great concern to me in my role as Executive Branch CITO. Problems with the cost-effective delivery of services, as well as with a delay in their implementation, mean that citizens are not receiving what they paid for, often at significant cost. They also consume inordinate and unplanned amounts of time for staff and management, resources that are usually taken away from where they are appropriately devoted, the accomplishment of the people's business.

However, despite our track record at the state, there are inevitably going to be troubled projects. Such problems are not unique to the public sector, however. In 2009, the Standish Group found that only 32% of all IT projects are delivered on-time, on budget, with required features and functions. To address these problems, most organizations have implemented similar project management oversight to the approach we make use of at the state, one based on the framework established by Senate Bill 5 in 1998. In addition, the private sector also makes use of another industry practice, the engagement of Independent Verification and Validation (IV&V) services by independent private sector contractors with experience in the specific domain in which the project is being conducted. IV&V is a professional software and systems engineering discipline and governed by an international standard.

The use of private IV&V contractors to perform independent IT audits of the type contemplated in SB 2 is not new to the state. Information Technology Executive Council (ITEC) Policy 2510 titled "Oversight of Information Technology Projects" specifies, in part:

6.1 All information technology projects will be conducted under the oversight of the entity executive management.

*6.2 The Branch CITO, when reviewing projects that are subject to CITO review, will evaluate the size, complexity, risk and consequences of failure for proposed projects **and will determine to what extent IV&V oversight will be required to adequately monitor the execution of entity information technology projects.** At a minimum, large projects over $10.0 million in a three-year life cycle will be required to engage external IV&V on the project. The IV&V assessment will be submitted directly and simultaneously to the Project Sponsor and the Branch CITO. **The IV&V assessment will also be made available to the Legislative CITO, entity head and project manager.***

The scope and contracting for such services is conducted in partnership with the Kansas Information Technology Office, a support group to the three branch CITOs that works with state agencies to orchestrate the project planning and oversight process on an ongoing basis. As the work is performed, reports are provided directly to the Executive Branch CITO along with the agency executives associated with the project, so that judgments about the project's health and any needed corrections can be reviewed by an independent party that can require such actions by the project to improve its health.

The use of this approach addresses a number of challenges to the in-house assessment by the Legislative Division of Post Audit contemplated in SB 2. Foremost, it allows the state to avail itself of the skills of private sector professionals with deep experience in the particular domain in which the project is being implemented. While some risks associated with projects are generic, there is tremendous value in bringing to bear the expertise of auditors familiar with a specific type of project in a particular program or industry as they assess project risks and performance on an ongoing basis. Such assessments involve application of not only knowledge and experience in technology and software design processes, but also organizational change, project, and financial management. The second challenge addressed by contracting for the use of private sector IV&V is the fact that schedules across agencies and projects may not often align with the availability of the finite number of LPA staff that would be charged with performing the ongoing assessment. It is possible that a number of projects may kick off, or engage in high-intensity phases that are fraught with risk at almost the same time. And, when/if problems are found, additional time will undoubtedly be required for discussions regarding the remediation steps required in situations that may involve analyzing complex tradeoffs under a deadline, with potentially significant cost implications for delay.

In both these situations, the limitations inherent in an in-house audit approach would present significant challenges. In contrast, private sector IV&V services can supply experienced resources to match the demand, with their availability specifically tailored to the timing and risks associated with each project, ensuring that assessment does not need to be prioritized across those state auditing resources available.

To summarize, I support the provisions of the bill related to security audits and appreciate the fine work that the Legislative Division of Post Audit performs on a daily basis in partnership with the Executive Branch. However, while I support the theory of increased external audit of IT projects at the state, I recommend an alternative approach to the Committee for its consideration that I believe will be more effective, enable us to take direct advantage of highly skilled private sector professionals in this domain, and avoid some of the learning curve and potential limitations associated with increasing this effort in-house.

For the reasons I've outlined previously, I recommend to the committee that rather than statutorily charging the Legislative Division of Post Audit with performing continuous audits of IT projects, my office will expand the requirement for external private sector IV&V to be conducted on additional projects, coupling it with a risk assessment that can be used to make decisions to apply it based on cost-benefit. I welcome the chance to work with the Legislative Division of Post Audit to draft and review criteria for its application under ITEC Policy 2510, as well as to share the results of such reporting with the Legislative Chief Information Technology Officer or with legislative committees as you direct. I believe that this approach best addresses the ongoing monitoring of risk, while strengthening the existing IT governance structure already established by the Legislature and increasing the effectiveness of its project management controls.

Thank you for your time and consideration of my recommendations. I will be happy to stand for questions.