MEMORANDUM

Legislative Division of Post Audit
800 SW Jackson, Suite 1200
Topeka, KS 66612-2212
voice: 785.296.3792
fax: 785.296.4482
web: www.kslpa.org

TO: Members, Senate Ways & Means Committee
FROM: Scott Frank, Legislative Post Auditor
DATE: January 26, 2016
SUBJECT: Testimony Supporting Senate Bill 313

I appreciate the opportunity to testify in favor of Senate Bill 313, which would amend the Legislative Post Audit Act by limiting the reporting provisions for our information technology audits.

Background Information

The 2015 Legislature passed House Bill 2010 which included two key information technology provisions. First, as a response to one of our recommendations in a December 2013 performance audit of the Office of Information Technology Services (OITS), the bill established OITS as a separate state agency for budgetary purposes. Second, the bill established a new category of audits in the Legislative Post Audit Act—information technology audits. The bill currently before you would limit the reporting provisions associated with these information technology audits.

K.S.A. 46-1135 (i.e., the IT audit provisions of House Bill 2010) requires our office to conduct information technology audits at the direction of the Legislative Post Audit Committee. This includes two types of audits: (1) IT security audits and (2) IT project audits. The first type –IT security audits—examines the controls agencies place around their most sensitive data systems and provides the agencies with a detailed technical report listing the security vulnerabilities our auditors identify. The second type—IT project audits—involve continuous monitoring of ongoing IT projects, looking for signs that the project is at risk of failure.

Provisions of Senate Bill 313

K.S.A. 46-1135 requires written reports on the results of both types IT audits be provided to several groups, including the agency being audited, the Governor, the three chief information technology officers (CITOs), the Legislative Post Audit Committee, and the Joint Committee on Information Technology (JCIT). We have no concerns with the reporting provisions as they apply to the IT project audits, as these reports will be publicly available anyway. However, we are concerned about making a wide distribution of the technically detailed IT security audits, which are kept confidential to as to not help a potential hacker.

Senate Bill 313 would limit the distribution of the confidential IT security audits to the agency, the appropriate branch CITO, the Post Audit Committee, and the JCIT. These are the groups that we have typically shared our IT security findings with in the past. We would continue to notify the other branch CITOs and the Governor that a report has been issued, but would not automatically make those reports available to them.