AUDIT PROPOSAL

State Agency Information Systems:
Reviewing Security Controls in Selected State Agencies (CY 2017-2019)

SOURCE

This audit proposal was suggested by LPA staff to satisfy requirements in K.S.A. 46-1135.

BACKGROUND

It is important that state agencies security measures are periodically evaluated to help ensure the safety of the sensitive data they maintain. Many state agencies collect and process millions of sensitive records in their computer systems, including individuals' social security numbers, medical and financial and tax information. Additionally, several agencies process payments including paychecks, unemployment, or child care assistance benefits. This makes those state agencies an enticing target for hackers. Although agencies often use multiple security layers to protect data and computers from cyber or physical attacks including locked doors, employee badges, network firewalls, and user passwords, these controls should be evaluated periodically to ensure the agency's sensitive data is sufficiently protected from accidental or intentional data breaches.

Currently, there is limited oversight of agencies' security controls to ensure that agencies are adequately protecting confidential data. The Kansas Information Technology Executive Council (ITEC) has developed standards across several security areas including security awareness training, access controls, and physical and environmental safeguards. These standards were created to ensure state agencies develop adequate security controls. However, agencies have a significant amount of autonomy in how they develop, apply, and monitor these security controls.

The 2015 Legislature passed K.S.A. 46-1135, which directs our office to conduct information technology audits as directed by the Legislative Post Audit Committee. Those audits are to include an assessment of the security practices at state agencies or any other entities subject to audit under the Legislative Post Audit Act. These audits are conducted on a three-year cycle. The current cycle (2017 – 2019) began with a statewide assessment of what types of sensitive datasets the state maintains and which agencies are responsible for those data.

AUDIT OBJECTIVES AND TENTATIVE METHODOLOGY

The audit objectives listed below represent the questions that we would answer through our audit work. The proposed steps below each objective are intended to convey the type of work we would do, but are subject to change as we learn more about the audit issues and are able to refine our methodology.

Objective 1: Do selected agencies adequately comply with applicable information technology security standards and employ adequate controls for emerging technologies? Our tentative methodology would include the following:

- Select agencies to be audited based on our statewide risk assessment and other factors including previous audit coverage and findings.

- Identify and create a list of applicable IT requirements from ITEC or other relevant standard-setting bodies for major security areas to evaluate.

- Ask officials of selected agencies to be audited to self-assess their compliance with those state requirements and other security standards and assess agency reported compliance through an onsite review that would consist of reviewing policies, employee training records, screenshots, and other relevant documentation.

- Select a sub-set of specific security requirements and evaluate a sample of each agency's high-risk computer systems, to ensure their system controls worked correctly.

- Interview agency officials and staff as needed to understand any compensating controls agencies have implemented to adequately cover areas in which they do not follow ITEC or other relevant security standards.

ESTIMATED RESOURCES

These audits will be conducted by our **four (4)** person information technology audit team.