AUDIT PROPOSAL

Information Systems:
Reviewing Significant Security Controls in Selected State and Local Agencies (CY 2020-2022)

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

BACKGROUND
Many state agencies and other local subdivisions of government collect and process millions of sensitive records in their computer systems, including individuals' social security numbers, medical and financial records, tax information, and student information. Additionally, several government entities process payments including paychecks, unemployment, or childcare assistance benefits. Government entities 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. While these measures are good, they should be evaluated periodically to ensure the entity's sensitive data is sufficiently protected from accidental or intentional data breaches.

Currently, there is limited oversight of government entities' security controls to ensure they 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. Additionally, other national and international security standards are available for entities to evaluate to secure their environments. Government entities 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 local subdivision of government receiving funding from or through the state. These audits are conducted on a three-year cycle.

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 state and local entities adequately comply with significant information technology security standards and best practices? Our tentative methodology would include the following:

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

- Identify and create a list of significant IT requirements from the Kansas Information Technology Executive Council (ITEC) and best practices from other relevant standard-setting bodies to evaluate.

- Assess entity compliance through reviewing employee training and other records, testing computer vulnerability remediation processes, reviewing access control and boundary information, observing physical security compliance, interviewing IT and other staff, and other work as applicable.

- Select a high-risk computer system the entity manages and evaluate its compliance with a limited number of specific security requirements or best practices.

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

ESTIMATED RESOURCES

These audits will be conducted by our 3-person information technology audit team.