AUDIT PROPOSAL

Availability, Cost, and Quality of Centralized IT Security Services

SOURCE

This audit proposal was suggested by LPA staff to satisfy committee rule 1-5(c).

BACKGROUND

The 2013 Legislature established the Office of Information Technology Services (OITS) as the state's central IT services agency.

OITS has been gradually moving to a consolidated services model. Under that model, it has consolidated state IT infrastructure and outsourced some services to third party vendors. This model is intended to minimize risk, reduce cost, and improve the reliability of state IT systems. Our 2019 of IT consolidation that showed it will likely increase the state's IT costs, but mostly because it will require the state to update very old IT infrastructure across cabinet level agencies. The audit also highlighted concerns about the responsiveness and quality of the consolidated services provided by OITS.

In 2018, the Legislature enacted the Cybersecurity Act. This Act aimed to reduce the risk of cybersecurity breaches. Among other things, it created the Kansas Information Security Office (KISO) to administer the Act. The KISO provides IT security services to state agencies and charges those agencies. KISO's fiscal year 2022 budget request was almost $5.4 million.

Recent IT security audits we've conducted found agencies' do not have necessary IT staff and assets to maintain a strong security posture. These audits also raised questions about whether IT security services provided through OITS and KISO are sufficiently available, comprehensive, high quality, and cost effective.

AUDIT OBJECTIVES AND TENTATIVE METHODOLOGY

The audit objectives listed below are the questions we would answer through our audit work. The steps listed for each objective convey the type of work we would do. These may change as we learn more about the audit issues.

Objective 1: Are the IT security services offered through OITS and KISO sufficiently comprehensive to meet statutory requirements and state agencies' needs? Our tentative methodology would include the following:

- Review applicable documents and interview officials to understand what IT security services OITS and KISO provide to comply with the Cybersecurity Act.

- Review applicable documents and interview officials what IT security services OITS and KISO offer to state agencies.

- Review the state's security requirements for state agencies and compare them to the list of IT security services offered by OITS and KISO to determine if any gaps exist.

- Interview OITS and KISO officials, agency officials, and others as necessary to determine how any gaps in services we identify affect state agencies' ability to meet their IT security needs.

Objective 2: Do OITS and KISO provide high quality and cost-effective IT security services to state agencies? Our tentative methodology would include the following:

- Survey agency officials to collect their opinions on the quality and cost of IT security services provided by OITS and KISO.
- Review a sample of services provided to determine if they were provided timely, in accordance with any relevant agreements, and were sufficient to meet security standards.
- Work with OITS and KISO officials to understand how general and specific security-service fees or rates (and indirect costs as applicable) were established or revised since the Cybersecurity Act went into effect.
- Interview selected agency officials to understand whether they think the fees they pay to OITS and KISO are reasonable, and if not why not.
- Request internal documents and analyze any cybersecurity fees OITS and KISO collected since July 2018 by agency and service type, as feasible. Compare those fees to the costs incurred by OITS and KISO to provide them.

ESTIMATED RESOURCES

We estimate this audit would require a team of **3 auditors** for a total of **3 months** (from the time the audit starts to our best estimate of when it would be ready for the committee).