Kansas Information Security Office
2800 SW Topeka Blvd., Building 100
Topeka, KS 66611

Kansas
Office of Information Technology Services

Phone: (785) 296-0814
kiso.ks.gov

DeAngela Burns-Wallace, Chief Information Technology Officer
Jeff Maxon, Chief Information Security Officer

Laura Kelly, Governor

TO: **Unemployment Compensation Modernization and Improvement Council**

FROM: **Jeff Maxon, Chief Information Security Officer, Kansas Information Security Office**

DATE: **September 19, 2022**

RE: **Protection of Cybersecurity Audits and Assessments from Kansas Open Records**

The BKD/FORVIS cybersecurity audit should remain confidential and protected from open and public discussion due to K.S.A. 45-221(a)(12) and (45), because release of the information could jeopardize the agency's cybersecurity posture. As referenced below, this statute explicitly calls out the protection of records related to cybersecurity plans, cybersecurity assessments, and cybersecurity vulnerabilities. This statute is the same statute that the Legislative Division of Post Audit uses to protect their cybersecurity audits from public discussion. KDOL recently went through an LPA Security Audit that was presented to Legislative Post Audit Committee in Executive Session on the 20th of July.

Publicly discussing the results of an identified agency's cybersecurity audit, assessment, or identified cybersecurity vulnerabilities could expose the agency to undue risk. State of Kansas entities are under constant attack from malicious cyber actors. Many of these threat actors spend time researching their targets and crafting their attacks based on publicly available information. Steps should be taken to not provide these threat actors with additional information that could be used or leveraged to compromise an agency's network resulting in a disruptive attack or data breach.

K.S.A. 45-221: Certain records not required to be open; separation of open and closed information required; statistics and records over 70 years old open.

(a)(12) Records of emergency or security information or procedures of a public agency, if disclosure would jeopardize public safety, including records of cybersecurity plans, cybersecurity assessments and cybersecurity vulnerabilities or procedures related to cybersecurity plans, cybersecurity assessments and cybersecurity vulnerabilities, or plans, drawings, specifications or related information for any building or facility that is used for purposes requiring security measures in or around the building or facility or that is used for the generation or transmission of power, water, fuels or communications, if disclosure would jeopardize security of the public agency, building or facility.

(a)(45) Records, other than criminal investigation records, the disclosure of which would pose a substantial likelihood of revealing security measures that protect: (A) Systems, facilities or equipment used in the production, transmission or distribution of energy, water or communications services; (B) transportation and sewer or wastewater treatment systems, facilities or equipment; or (C) private property or persons, if the records are submitted to the agency. For purposes of this paragraph, security

means measures that protect against criminal acts intended to intimidate or coerce the civilian population, influence government policy by intimidation or coercion or to affect the operation of government by disruption of public services, mass destruction, assassination or kidnapping. Security measures include, but are not limited to, intelligence information, tactical plans, resource deployment and vulnerability assessments.

Reference: http://ksrevisor.org/statutes/chapters/ch45/045_002_0021.html