FAQ for Cybersecurity Incident Reporting

Who does this law apply to?

- Any public entity that experiences a significant cybersecurity incident.
- Any government contractor that has a significant cybersecurity incident.

What are the reporting timeframes?

- Any **public entity** shall report within 12 hours after the discovery of the incident.
- Any **government contractor** that has a significant cybersecurity incident must report within:
    - 72 hrs. after the government contractor reasonably believes a significant cybersecurity incident has occurred; or
    - 12 hrs. if a determination is made during the investigation that such information, network or systems operated by or on behalf of the State were directly impacted.

What constitutes a 'significant cybersecurity incident'?

- A cybersecurity incident that results in or is likely to result in financial loss or demonstratable harm to public confidence or public health and safety in the State of Kansas. Any event or combination that threatens, without lawful authority the confidentiality, integrity or availability of information or information systems and that requires an entity to initiate a response or recovery. Examples include but are not limited to malware, ransomware, denial of service, man in the middle and other such attacks by bad actors.

Examples:

What to report:

- Denial of service attack that lasted over an hour.
- Discovery of ransomware note
- Multiple anti-virus or endpoint detection and response alerts resulting in a need to contain or shutdown systems.

Things not to report:

- Individual phishing message
- Single anti-virus alerts

If the event happens on a Kansas Criminal Justice Information System (KCJIS) machine or system, do I still report it to the KISO?

- No, if the incident is on KCJIS equipment you will follow the same reporting process that you have always had, and the Kansas Bureau of Investigation (KBI) will make the necessary notification to the KISO within the prescribed timeframe.

If the incident impacts the election equipment or systems, do I still report it to the KISO?

- Yes, if the incident involves the election equipment or systems you will report it to the KISO and to the Kansas Secretary of State's Office within the prescribed time frames.

Is my report protected?

- Yes, the reported incident will only be shared internally to those needing to assist in handling of the incident and the incident is protected from the open records act. The only reporting on state incidents that will be done is anonymized in aggregate reporting.

How do I make a report of an incident?

- You can report an incident one of two ways:
    1. You can call 785-296-6069 which will be monitored and/or answered 24/7.
    2. Complete the report form on the KISO Website at: KISO Home https://ebit.ks.gov/kiso/home by clicking on the yellow "Report Security Incident" button.

What information needs to be reported?

You will need to provide:

- Status of the incident
- A point of contact for the entity experiencing the incident
- Where the incident occurred and time it was discovered.

- Additional information about how the incident was detected, if it has been resolved, and who all has been notified.
- The impact of the incident, criticality of the incident, and actions that have been taken.
- Finally, if you are needing assistance with containment, mitigation, investigation, or remediation.

Why do I have to report this to the KISO?

- The Kansas Information Security Office has been designated by the Kansas Legislature as the point of contact for reporting and/or coordination of assistance for any incidents that could potentially threaten state systems. The KISO is also committed to assisting public entities and providing resources to assist with handling the incident.

My cyber insurance company says I cannot notify anyone if I have an incident. Do I still have to report?

- Yes, this is State Law, insurance policies cannot violate state law. If your policy includes language to this effect, please contact your insurance company and make sure they are aware of the State Law and if necessary, amend the language in your policy.