SUBJECT: Prohibiting certain social media applications on state-owned devices

COMMITTEE: State Affairs — committee substitute recommended

VOTE: 9 ayes — Hunter, Hernandez, Dean, Geren, Guillen, Metcalf, Slawson, Smithee, Spiller

0 nays

4 absent — Anchía, Raymond, S. Thompson, Turner

WITNESSES: For — (*Registered, but did not testify*: Thomas Parkinson)

Against — (*Registered, but did not testify*: Tez Figueroa)

On — (*Registered, but did not testify*: Matthew Kelly, Department of Information Resources; Shawn Hall Lecuona, Kri'ah b'shalom)

BACKGROUND: Some have suggested that adopting a policy on prohibited applications could help protect the state from potential security risks posed by certain social media services and applications.

DIGEST: HB 3289 would require state agencies to adopt a policy prohibiting the installation or use of a prohibited application on any device owned or leased by the state agency, and would require the removal of prohibited applications from those devices. The Department of Information and Resources (DIR) and the Department of Public Safety (DPS) would be required to jointly develop a model policy for state agencies for use regarding the required policy.

HB 3289 would define a "prohibited application" as a social media application or service that appeared on the list of security threats published by DIR as established by the bill, or a social media application that the governor had identified as a security threat by executive order.

The policy adopted by these agencies could include an exception allowing

the installation and use of a prohibited application to the extent necessary for:

- providing law enforcement;
- developing or implementing information security measures; and
- allowing other legitimate governmental uses as jointly determined by DIR and DPS.

A policy allowing the installation of and use of a prohibited application would require the use of measures to mitigate risks to the security of state agency information during the use of prohibited applications and documentation of those measures.

The administrative head of a state agency would be required to approve in writing the installation and use of a prohibited application under the exceptions above by its employees and report the approval to DIR.

The governor would could by executive order identify social media applications or services that posed a threat to the security of the state's sensitive information, critical infrastructure, or both.

DIR and DPS, in consultation with the governor, would be required to identify social media applications or services that posed a threat to security. DIR would annually publish and maintain a list of prohibited applications on its website in a publicly accessible format.

Each state agency would be required to adopt the model policy no later than 60 days after DPS made the policy available.

This bill would take immediate effect if finally passed by a two-thirds record vote of the membership of each house. Otherwise, it would take effect September 1, 2023.