BILL ANALYSIS

C.S.H.B. 3289
By: Anderson
State Affairs
Committee Report (Substituted)

BACKGROUND AND PURPOSE

Governor Abbot, members of the U.S. Congress, and the FBI have all expressed concerns over the potential security risks posed by the use of TikTok. In December 2022, Governor Abbott ordered that all state agencies prohibit the use of TikTok on any government-issued devices. C.S.H.B. 3289 seeks to establish a formal state policy on the use of social media services and applications such as TikTok that pose potential security risks to the state by requiring all state agencies to adopt policies prohibiting the use of certain services and applications identified as posing potential such security risks on any devices owned or leased by the agency, with certain authorized exceptions, including for law enforcement purposes.

CRIMINAL JUSTICE IMPACT

It is the committee's opinion that this bill does not expressly create a criminal offense, increase the punishment for an existing criminal offense or category of offenses, or change the eligibility of a person for community supervision, parole, or mandatory supervision.

RULEMAKING AUTHORITY

It is the committee's opinion that this bill does not expressly grant any additional rulemaking authority to a state officer, department, agency, or institution.

ANALYSIS

C.S.H.B. 3289 amends the Government Code to require the Department of Information Resources (DIR) and the Department of Public Safety (DPS), in consultation with the governor's office, to jointly identify social media applications or services that pose a threat to the security of the state's sensitive information, critical infrastructure, or both. The bill requires DIR to publish annually and maintain on its publicly accessible website a list of the identified applications. The bill authorizes the governor by executive order to also identify social media applications or services that pose a threat to the security of the state's sensitive information, critical infrastructure, or both.

C.S.H.B. 3289 requires all state agencies to adopt a policy that prohibits the installation or use of the following prohibited applications on any device owned or leased by the agency and requiring the removal of such applications from those devices:

- a social media application or service included on the list published by DIR; or
- any other social media applications or services specified by an executive order of the governor.

The bill requires DIR and DPS to jointly develop a model policy for state agencies to use in developing their own policies and requires each state agency to adopt their policy not later than the 60th day after the model policy is made available.

C.S.H.B. 3289 authorizes an agency's policy to include an exception allowing for the installation and use of a prohibited application to the extent necessary for providing law enforcement, for

developing or implementing information security measures, or to allow other legitimate governmental uses as jointly determined by DIR and DPS. The bill requires a policy that allows such limited installation and use of a prohibited application to require the use of measures to mitigate risks to the security of state agency information during the use of the covered application and the documentation of those measures. The bill requires the administrative head of a state agency to approve in writing the installation and use of a prohibited application under an exception by agency employees and report the approval to DIR.

EFFECTIVE DATE

On passage, or, if the bill does not receive the necessary vote, September 1, 2023.

COMPARISON OF INTRODUCED AND SUBSTITUTE

While C.S.H.B. 3289 may differ from the introduced in minor or nonsubstantive ways, the following summarizes the substantial differences between the introduced and committee substitute versions of the bill.

The substitute expands the social media applications or services subject to the state agency policies. Whereas in the introduced these policies dealt with "covered applications," which were the social media service TikTok or its successors or provided by ByteDance Limited, as well as any social media application or service specified by executive order of the governor as posing a similar risk to the security of state agency information, the substitute makes these policies applicable instead with respect to any "prohibited applications," which include those identified by DIR and DPS as posing a threat to the security of the state's sensitive information, critical infrastructure, or both or specified by executive order of the governor as posing such a threat. Accordingly, the substitute includes provisions not in the introduced that require DIR and DPS, in consultation with the governor's office, to jointly identify social media applications or services that pose such a threat and require DIR to publish and maintain on its publicly accessible website a list of prohibited applications.

The substitute includes a provision not in the introduced that requires DIR and DPS to jointly develop a model policy for state agencies to use in developing their own policies. Whereas the introduced required each state agency to adopt the required policy not later than the 60th day after the bill's effective date, the substitute instead requires the policies to be adopted not later than the 60th day after DIR and DPS make the model policy available.

The substitute revises provisions in the introduced that authorized a state agency policy to include certain exceptions to its policy to include among the authorized exceptions an authorization that allows for the use and installation of a prohibited application to the extent necessary to allow other legitimate governmental uses as determined jointly by DIR and DPS. The substitute includes a provision not in the introduced requiring the administrative head of a state agency to approve in writing the installation and use of a prohibited application by employees of the state in accordance with an exception included in the agency's policy and to report such approval to DIR.