Date of Hearing: August 23, 2023

ASSEMBLY COMMITTEE ON APPROPRIATIONS
Chris Holden, Chair
SB 74 (Dodd) – As Amended August 17, 2023

Policy Committee: Accountability and Administrative Review Vote: 6 - 0

Urgency: Yes State Mandated Local Program: No Reimbursable: No

SUMMARY:

This bill requires state agencies, when implementing social media and cybersecurity policies and authorizing any installation or download of an application (app) for a particular social media platform on a state-issued or state-owned electronic device, to adopt risk mitigation strategies tailored to risks posed by that app.

This bill provides, for purposes of adopting these risk mitigation strategies, a rebuttable presumption that a state agency prohibits installation or download of an app meeting specified conditions involving an "entity of concern" or a "country of concern." A state agency can overcome the rebuttable presumption, if the state agency does all of the following:

1) Implements social media and cybersecurity policies in compliance with the Statewide Information Management Manual (SIMM).

2) Makes a written finding that installation or download of the app is necessary for an official state purpose.

3) Authorizes installation or download of the app only for the declared official state purpose and for no longer than necessary to complete that purpose.

4) Submits documentation of compliance with these requirements to the Department of Technology (CDT), prior to authorizing app installation or download.

A state agency with such an app already installed or downloaded on agency devices upon the effective date of this bill must submit the documentation of compliance within 30 calendar days.

FISCAL EFFECT:

1) Costs of an unknown, but likely significant, amount across state agencies to adopt specified risk mitigation strategies, which could include information technology (IT) resources to prohibit staff from accessing certain apps, and, if needed, submit documentation of compliance to CDT to overcome the rebuttable presumption to use certain apps for an official state purpose.

2) Annual costs of approximately $1.5 million to CDT for five positions and a contract with a vendor specializing in mobile apps to ensure oversight of state agencies' risk mitigation

strategies, including performing ongoing social media risk analysis for countries of concern and reviewing rebuttable presumption compliance documentation.

COMMENTS:

1) **Purpose.** According to the author:

> Prohibiting high-risk apps on state phones and other devices is a commonsense way to prevent exposure of our sensitive material and the possible tracking or data breaches. Clearly there are bad actors out there, and we can't afford to let them in.

2) **Support, Opposition, and Recent Amendments.** This bill is supported by the Consumer Federation of California, which argues "data breaches are a threat not only to consumers but also to state agencies…At least two dozen states have instituted some type of limitation on the use of high-risk apps on state-controlled or provided devices."

   There is no registered opposition on file to this bill. However, TikTok, Inc. requested amendments to the prior version of this bill for "a more comprehensive approach; specifically, amendments which would prohibit all types of entertainment and social media platforms or [apps] from being downloaded or installed on state-owned devices." Amendments adopted to this bill by the Assembly Accountability and Administrative Review Committee modified the approach of this bill to provide a rebuttable presumption that certain apps are prohibited pursuant to risk mitigation strategies, rather than imposing a direct prohibition on certain apps. However, this bill still centers on apps connected to a "country of concern," rather than all apps generally.

3) **Existing Social Media Policy for State Agencies.** CDT oversees the SIMM, which includes standards, instructions, forms, and templates that state agencies must use to comply with state IT policy consistent with the SIMM. The SIMM's "Social Media Standard" encourages state agencies to use social media to engage customers and employees where appropriate, subject to risk mitigation. Before authorizing and enabling internet access from a state device to any social media platform, the SIMM requires each state agency to conduct a formal risk assessment and identify mitigation strategies for risks, including potential "exposure or leakage of sensitive or protected information" and "malware introduction into the organization's IT environment." A state agency can allow connection to only social media platforms authorized by agency management.

   This bill requires state agencies, when authorizing any installation or download of an app for a particular social media platform on a state-issued or state-owned electronic device, to adopt risk mitigation strategies tailored to risks posed by that app and provides a rebuttable presumption that a state agency's risk mitigation strategy prohibits installation or download of an app meeting specified conditions involving an "entity of concern," meaning a company domiciled or organized in a "country of concern." Although many countries meet the definition of "country of concern" provided by this bill, including Cuba, Iran, and North Korea, this bill is generally understood to be a response to TikTok, owned by ByteDance, a company based in China, that the Federal Bureau of Investigation states could be used by the Chinse Communist Party to exploit Americans' user data for espionage operations, control Americans' mobile device software, and manipulate content for influence operations.

Analysis Prepared by: Irene Ho / APPR. / (916) 319-2081