

AMENDED IN ASSEMBLY AUGUST 17, 2023

AMENDED IN SENATE MAY 18, 2023

AMENDED IN SENATE APRIL 26, 2023

AMENDED IN SENATE APRIL 10, 2023

AMENDED IN SENATE MARCH 22, 2023

AMENDED IN SENATE FEBRUARY 14, 2023

SENATE BILL

No. 74

Introduced by Senators Dodd and Jones

(Principal coauthor: Assembly Member Sanchez)

**(Coauthors: Senators Grove, Hurtado, Min, Nguyen, Niello,
Ochoa Bogh, Portantino, and Skinner)**

(Coauthors: Assembly Members Jackson and Mathis)

January 11, 2023

An act to add Section 11547.6 to the Government Code, relating to technology, and declaring the urgency thereof, to take effect immediately.

LEGISLATIVE COUNSEL'S DIGEST

SB 74, as amended, Dodd. State entities: state-owned or state-issued devices: social media platforms.

Existing law establishes the Department of Technology (department) within the Government Operations Agency, and provides for a Director of Technology (director) to supervise the department and report directly to the Governor on issues relating to information technology. Existing law imposes various duties on the director, including advising the Governor on the strategic management and direction of the state's

information technology resources. Existing law requires the department to identify, assess, and prioritize high-risk, critical information technology services and systems across state government, as determined by the department, for modernization, stabilization, or remediation.

Existing law requires the Office of Emergency Services to establish and lead the California Cybersecurity Integration Center (CCIC). Existing law states that the CCIC's mission is to reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector computer networks in the state. Existing law requires the CCIC to serve as the central organizing hub of state government's cybersecurity activities and coordinate information sharing with specified entities, including local, state, and federal agencies.

~~This bill, except as specified, would require state entities to prohibit applications for social media platforms from being downloaded or installed on those entities' state-owned or state-issued devices if specified conditions are met, including that an entity of concern or a country of concern directly or indirectly owns, directly or indirectly controls, or holds 10% or more of the voting shares of the social media company that owns the application.~~ *bill would require state agencies, when implementing social media and cybersecurity policies pursuant to the Statewide Information Management Manual and authorizing any agency installation or download of an application for a particular social media platform on a state-issued or state-owned electronic device for an official state purpose, to adopt risk mitigation strategies tailored to risks posed by that social media platform, as specified. For purposes of adopting these risk mitigation strategies, the bill would specify that there is a rebuttable presumption that a state agency shall prohibit installation or download on that agency's state-issued or state-owned electronic devices of any application for a social media platform to which any of specified conditions apply, and would specify how that rebuttable presumption may be overcome by the state agency. The bill would define various terms for these purposes.*

The bill would declare that it is to take effect immediately as an urgency statute.

Vote: $\frac{2}{3}$. Appropriation: no. Fiscal committee: yes.
State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Section 11547.6 is added to the Government Code, to read:

11547.6. (a) For purposes of this section, the following definitions apply:

(1) “Country of concern” means a country identified by the International Traffic in Arms Regulations as set forth in Section 126.1 of Part 126 of Title 22 of the Code of Federal Regulations.

(2) “Entity of concern” means a company that is domiciled in, is headquartered in, has its principal place of business in, or is organized under the laws of, a country of concern.

(3) “Social media company” has the same meaning as defined in Section 22675 of the Business and Professions Code.

(4) “Social media platform” has the same meaning as defined in Section 22675 of the Business and Professions Code.

~~(5) “State entity” means an entity within the executive branch that is under the direct authority of the Governor, including, but not limited to, all departments, boards, bureaus, commissions, councils, and offices.~~

~~(b) Except as specified in subdivision (c), a state entity shall prohibit an application for a social media platform from being installed or downloaded on that entity’s state-issued or state-owned electronic device if any of the following conditions are met:~~

~~(5) “State agency” means a state agency that is subject to the Statewide Information Management Manual.~~

~~(b) When implementing social media and cybersecurity policies pursuant to the Statewide Information Management Manual and authorizing any agency installation or download of an application for a particular social media platform on a state-issued or state-owned electronic device for an official state purpose, a state agency shall adopt risk mitigation strategies tailored to risks posed by that application for a social media platform.~~

~~(c) For purposes of adopting risk mitigation strategies pursuant to this section, there is a rebuttable presumption that a state agency shall prohibit installation or download on that agency’s state-issued or state-owned electronic devices of any application for a social media platform to which any of the following apply:~~

~~(1) An entity of concern or a country of concern directly or indirectly owns, directly or indirectly controls, or holds 10 percent~~

1 or more of the voting shares of the social media company that
2 owns the ~~application~~. *social media platform*.

3 (2) An entity of concern or a country of concern has substantial
4 direct or indirect influence over the social media company that
5 owns the social media platform, including, but not limited to, either
6 of the following:

7 (A) The entity of concern or country of concern could compel
8 the social media company to share data on a user that is a citizen
9 of this state with the entity of concern or the country of concern.

10 (B) The entity of concern or country of concern has substantial
11 influence over the content moderation practices of the social media
12 company.

13 (3) The social media platform uses software or an algorithm
14 controlled by a country of concern.

15 ~~(c) This section does not prohibit an application for a social~~
16 ~~media platform from being installed or downloaded on a state~~
17 ~~entity's state-issued or state-owned electronic device if the state~~
18 ~~entity uses that application for official state purposes, including,~~
19 ~~but not limited to, any of the following:~~

20 ~~(1) Official communications to the public on behalf of the state~~
21 ~~entity.~~

22 ~~(2) Cybersecurity research.~~

23 ~~(3) Law enforcement activities.~~

24 ~~(d) A state agency may overcome the rebuttable presumption~~
25 ~~in subdivision (c) only if the state agency does all of the following~~
26 ~~with respect to each application for a social media platform to~~
27 ~~which the rebuttable presumption applies:~~

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

30 ~~(2) Makes a written finding that installation or download of the~~
31 ~~application for the social media platform is necessary for an~~
32 ~~official state purpose.~~

33 ~~(3) Authorizes installation or download of the application for~~
34 ~~the social media platform only for the purpose described in~~
35 ~~paragraph (2) and for no longer than necessary to complete that~~
36 ~~purpose.~~

37 ~~(4) Prior to authorizing installation or download of the~~
38 ~~application for the social media platform, submits documentation~~
39 ~~of compliance with this section to the Department of Technology,~~
40 ~~which shall be available upon request by the Speaker of the~~

1 *Assembly or the President pro Tempore of the Senate. A state*
2 *agency that already has installed or downloaded on that agency's*
3 *state-issued or state-owned electronic devices an application for*
4 *a social media platform to which the rebuttable presumption*
5 *described in subdivision (c) applies on the effective date of this*
6 *section shall submit the documentation of compliance to the*
7 *Department of Technology within 30 calendar days of the effective*
8 *date of this section.*

9 SEC. 2. This act is an urgency statute necessary for the
10 immediate preservation of the public peace, health, or safety within
11 the meaning of Article IV of the California Constitution and shall
12 go into immediate effect. The facts constituting the necessity are:

13 In order to protect against imminent threats to data security, it
14 is necessary that this act take effect immediately.