

A-Engrossed
House Bill 3127

Ordered by the House March 24
Including House Amendments dated March 24

Sponsored by Representatives BOWMAN, EVANS, Senator KNOPP, Representatives HELFRICH, LEVY E, Senator WOODS; Representatives CONRAD, DEXTER, HIEB, LEWIS

SUMMARY

The following summary is not prepared by the sponsors of the measure and is not a part of the body thereof subject to consideration by the Legislative Assembly. It is an editor's brief statement of the essential features of the measure.

Identifies certain covered vendors. Directs State Chief Information Officer to adopt rules pertaining to designation of corporate entity as additional covered vendor for purposes of protecting state information technology assets.

Prohibits installation or download of [*certain*] covered products onto state information technology assets. Prohibits use or access of [*certain*] covered products by state information technology assets.

Requires state agencies to remove covered products from state information technology assets and implement all measures necessary to prevent installation or download of [*certain*] covered products onto state information technology assets and use or access of [*certain*] covered products by state information technology assets.

Permits state agency to permit download, installation, use or access of covered product for [*purpose of carrying out law enforcement activities*] **investigatory, regulatory or law enforcement purposes**. Requires state agency that permits download, installation, use or access of covered product to adopt risk mitigation standards and procedures.

Requires Secretary of State and State Treasurer to prohibit covered products of certain covered vendors from being installed or downloaded onto, or used or accessed by, state information technology assets, remove covered products installed or downloaded onto state information technology assets and implement all measures necessary to prevent installation or download of covered products onto, and use or access of covered products by, state information technology assets.

Permits Secretary of State or State Treasurer to permit download, installation, use or access of covered product for investigatory, regulatory or law enforcement purposes if Secretary of State or State Treasurer adopts risk mitigation standards and procedures.

Takes effect on 91st day following adjournment sine die.

A BILL FOR AN ACT

Relating to the security of state assets; and prescribing an effective date.

Be It Enacted by the People of the State of Oregon:

SECTION 1. As used in sections 1 to 3 of this 2023 Act:

(1) **“Covered product” means any form of hardware, software or service provided by a covered vendor.**

(2) **“Covered vendor” means any of the following corporate entities, or any parent, subsidiary, affiliate or successor entity of the following corporate entities:**

(a) **Ant Group Co., Limited.**

(b) **ByteDance Limited.**

(c) **Huawei Technologies Company Limited.**

(d) **Kaspersky Lab.**

(e) **Tencent Holdings Limited.**

(f) **ZTE Corporation.**

NOTE: Matter in **boldfaced** type in an amended section is new; matter [*italic and bracketed*] is existing law to be omitted. New sections are in **boldfaced** type.

1 (g) Any other corporate entity designated a covered vendor by the State Chief Informa-
2 tion Officer under section 3 of this 2023 Act.

3 (3) "State agency" means any board, commission, department, division, office or other
4 entity of state government, as defined in ORS 174.111, except that state government does not
5 include the Secretary of State or State Treasurer.

6 (4) "State information technology asset" means any form of hardware, software or ser-
7 vice for data processing, office automation or telecommunications used directly by a state
8 agency or used to a significant extent by a contractor in the performance of a contract with
9 a state agency.

10 **SECTION 2.** (1) A covered product may not be:

11 (a) Installed or downloaded onto a state information technology asset; or

12 (b) Used or accessed by a state information technology asset.

13 (2) A state agency shall:

14 (a) Remove any covered product that is installed or downloaded onto a state information
15 technology asset that is under the management or control of the state agency; and

16 (b) Implement all measures necessary to prevent the:

17 (A) Installation or download of a covered product onto a state information technology
18 asset that is under the management or control of the state agency; or

19 (B) Use or access of a covered product by a state information technology asset that is
20 under the management or control of the state agency.

21 (3)(a) Notwithstanding subsections (1) and (2) of this section, a state agency may, for
22 investigatory, regulatory or law enforcement purposes, permit the:

23 (A) Installation or download of a covered product onto a state information technology
24 asset; or

25 (B) Use or access of a covered product by a state information technology asset.

26 (b) A state agency that permits the installation, download, use or access of a covered
27 product under this subsection shall adopt risk mitigation standards and procedures related
28 to the installation, download, use or access of the covered product.

29 (4) The State Chief Information Officer shall coordinate with and oversee state agencies
30 to implement the provisions of this section in accordance with the policies and standards
31 adopted under section 3 (3) this 2023 Act.

32 **SECTION 3.** (1) The State Chief Information Officer shall adopt:

33 (a) Rules pertaining to the designation of a corporate entity as a covered vendor under
34 section 1 (2)(g) of this 2023 Act; and

35 (b) Policies and standards for state agencies to implement the provisions of section 2 of
36 this 2023 Act.

37 (2) The rules adopted under this section must include:

38 (a) The definition of "national security threat" for purposes of protecting state informa-
39 tion technology assets;

40 (b) Criteria and a process for determining when a corporate entity poses a national se-
41 curity threat; and

42 (c) Criteria and a process for determining when a corporate entity no longer poses a
43 national security threat.

44 (3) The policies and standards adopted under this section must include:

45 (a) The procedures for providing state agencies, the Secretary of State and the State

1 **Treasurer notice that a corporate entity is designated or no longer designated a covered**
2 **vendor under section 1 (2)(g) of this 2023 Act;**

3 **(b) The time schedules for implementing the requirements under section 2 of this 2023**
4 **Act with regard to a corporate entity that is designated a covered vendor by the State Chief**
5 **Information Officer; and**

6 **(c) The time schedules for incorporating the requirements under section 2 of this 2023**
7 **Act into a state agency's information security plans, standards or measures.**

8 **SECTION 4. (1) As used in this section:**

9 **(a) "Covered product" means any form of hardware, software or service provided by a**
10 **covered vendor.**

11 **(b) "Covered vendor" means any of the following corporate entities, or any parent, sub-**
12 **subsidiary, affiliate or successor entity of the following corporate entities:**

13 **(A) Ant Group Co., Limited.**

14 **(B) ByteDance Limited.**

15 **(C) Huawei Technologies Company Limited.**

16 **(D) Kaspersky Lab.**

17 **(E) Tencent Holdings Limited.**

18 **(F) ZTE Corporation.**

19 **(c) "State information technology asset" means any form of hardware, software or ser-**
20 **vice for data processing, office automation or telecommunications used directly by the office**
21 **of the Secretary of State or used to a significant extent by a contractor in the performance**
22 **of a contract with the office of the Secretary of State.**

23 **(2) Except as provided in subsection (4) of this section, the Secretary of State shall:**

24 **(a) Prohibit a covered product from being:**

25 **(A) Installed or downloaded onto a state information technology asset; or**

26 **(B) Used or accessed by a state information technology asset;**

27 **(b) Remove any covered product that is installed or downloaded onto a state information**
28 **technology asset; and**

29 **(c) Implement all measures necessary to prevent the:**

30 **(A) Installation or download of a covered product onto a state information technology**
31 **asset; or**

32 **(B) Use or access of a covered product by a state information technology asset.**

33 **(3) For any corporate entity that the State Chief Information Officer designates as a**
34 **covered vendor under section 3 of this 2023 Act, the secretary may:**

35 **(a) Prohibit a covered product from being:**

36 **(A) Installed or downloaded onto a state information technology asset; or**

37 **(B) Used or accessed by a state information technology asset;**

38 **(b) Remove any covered product that is installed or downloaded onto a state information**
39 **technology asset; and**

40 **(c) Implement all measures necessary to prevent the:**

41 **(A) Installation or download of a covered product onto a state information technology**
42 **asset; or**

43 **(B) Use or access of a covered product by a state information technology asset.**

44 **(4) If the secretary adopts risk mitigation standards and procedures related to the in-**
45 **stallation, download, use or access of a covered product, the secretary may, for**

1 investigatory, regulatory or law enforcement purposes, permit the:

2 (a) Installation or download of the covered product onto a state information technology
3 asset; or

4 (b) Use or access of the covered product by a state information technology asset.

5 **SECTION 5.** (1) As used in this section:

6 (a) "Covered product" means any form of hardware, software or service provided by a
7 covered vendor.

8 (b) "Covered vendor" means any of the following corporate entities, or any parent, sub-
9 sidiary, affiliate or successor entity of the following corporate entities:

10 (A) Ant Group Co., Limited.

11 (B) ByteDance Limited.

12 (C) Huawei Technologies Company Limited.

13 (D) Kaspersky Lab.

14 (E) Tencent Holdings Limited.

15 (F) ZTE Corporation.

16 (c) "State information technology asset" means any form of hardware, software or ser-
17 vice for data processing, office automation or telecommunications used directly by the office
18 of the State Treasurer or used to a significant extent by a contractor in the performance
19 of a contract with the office of the State Treasurer.

20 (2) Except as provided in subsection (4) of this section, the State Treasurer shall:

21 (a) Prohibit a covered product from being:

22 (A) Installed or downloaded onto a state information technology asset; or

23 (B) Used or accessed by a state information technology asset;

24 (b) Remove any covered product that is installed or downloaded onto a state information
25 technology asset; and

26 (c) Implement all measures necessary to prevent the:

27 (A) Installation or download of a covered product onto a state information technology
28 asset; or

29 (B) Use or access of a covered product by a state information technology asset.

30 (3) For any corporate entity that the State Chief Information Officer designates as a
31 covered vendor under section 3 of this 2023 Act, the State Treasurer may:

32 (a) Prohibit a covered product from being:

33 (A) Installed or downloaded onto a state information technology asset; or

34 (B) Used or accessed by a state information technology asset;

35 (b) Remove any covered product that is installed or downloaded onto a state information
36 technology asset; and

37 (c) Implement all measures necessary to prevent the:

38 (A) Installation or download of a covered product onto a state information technology
39 asset; or

40 (B) Use or access of a covered product by a state information technology asset.

41 (4) If the State Treasurer adopts risk mitigation standards and procedures related to the
42 installation, download, use or access of a covered product, the State Treasurer may, for
43 investigatory, regulatory or law enforcement purposes, permit the:

44 (a) Installation or download of the covered product onto a state information technology
45 asset; or

1 **(b) Use or access of the covered product by a state information technology asset.**
2 **SECTION 6.** **This 2023 Act takes effect on the 91st day after the date on which the 2023**
3 **regular session of the Eighty-second Legislative Assembly adjourns sine die.**
4
