Enrolled
House Bill 3127

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

CHAPTER .....

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.

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

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

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

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

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

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

(2) A state agency shall:

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

(b) Implement all measures necessary to prevent the:

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

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

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

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

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

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

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

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

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

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

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

(a) The definition of "national security threat" for purposes of protecting state information technology assets;

(b) Criteria and a process for determining when a corporate entity poses a national security threat; and

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

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

(a) The procedures for providing state agencies, the Secretary of State and the State Treasurer notice that a corporate entity is designated or no longer designated a covered vendor under section 1 (2)(g) of this 2023 Act;

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

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

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

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

(b) "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.

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

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

(a) Prohibit a covered product from being:

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

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

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

(c) Implement all measures necessary to prevent the:

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

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

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

(a) Prohibit a covered product from being:

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

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

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

(c) Implement all measures necessary to prevent the:

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

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

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

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

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

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

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

(b) "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.

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

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

(a) Prohibit a covered product from being:

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

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

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

(c) Implement all measures necessary to prevent the:

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

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

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

(a) Prohibit a covered product from being:

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

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

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

(c) Implement all measures necessary to prevent the:

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

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

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

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

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

SECTION 6. This 2023 Act takes effect on the 91st day after the date on which the 2023 regular session of the Eighty-second Legislative Assembly adjourns sine die.

Passed by House March 28, 2023

.....
Timothy G. Sekerak, Chief Clerk of House

.....
Dan Rayfield, Speaker of House

Passed by Senate June 21, 2023

.....
Rob Wagner, President of Senate

Received by Governor:

.....M.,....., 2023

Approved:

.....M.,....., 2023

.....
Tina Kotek, Governor

Filed in Office of Secretary of State:

.....M.,....., 2023

.....
Secretary of State