83rd OREGON LEGISLATIVE ASSEMBLY--2025 Regular Session

A-Engrossed

House Bill 3936

Ordered by the House May 12
Including House Amendments dated May 12

Sponsored by Representative EDWARDS

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. The statement includes a measure digest written in compliance with applicable readability standards.

Digest: Bans the use of AI on state assets if the AI is developed or owned by a covered vendor. (Flesch Readability Score: 80.6).

[*Digest: Bans the use of AI on state assets if the AI is owned or developed by a foreign corporate entity. (Flesch Readability Score: 68.0).*]

Prohibits any hardware, software or service that uses artificial intelligence from being installed or downloaded onto or used or accessed by state information technology assets if the artificial intelligence is developed or owned by a [*corporate entity that is incorporated or registered under the laws of a foreign country*] **covered vendor**. Provides for exceptions.

A BILL FOR AN ACT

Relating to the security of state assets; amending ORS 276A.340, 276A.344, 276A.346 and 276A.348.

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

SECTION 1. ORS 276A.340 is amended to read:

276A.340. As used in ORS 276A.340 to 276A.344:

(1) "Artificial intelligence" means a machine-based system that is capable, for a given set of human-defined objectives, of making predictions, recommendations or decisions influencing real or virtual environments and uses machine- or human-based inputs to:

(a) Perceive real or virtual environments;

(b) Abstract the perceptions into models through analysis in an automated manner; and

(c) Use model inference to formulate options for information or action.

[*(1)*] **(2)** "Covered product" means**:**

(a) Any form of hardware, software or service provided by a covered vendor.

(b) Any hardware, software or service that uses artificial intelligence and the artificial intelligence is developed or owned by a covered vendor.

[*(2)*] **(3)** "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 ORS 276A.344.

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.

[*(3)*] **(4)** "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)*] **(5)** "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. ORS 276A.344 is amended to read:

276A.344. (1) The State Chief Information Officer shall adopt:

(a) Rules pertaining to the designation of a corporate entity as a covered vendor under ORS 276A.340 [*(2)(g)*] **(3)(g)**; and

(b) Policies and standards for state agencies to implement the provisions of ORS 276A.342.

(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 ORS 276A.340 [*(2)(g)*] **(3)(g)**;

(b) The time schedules for implementing the requirements under ORS 276A.342 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 ORS 276A.342 into a state agency's information security plans, standards or measures.

SECTION 3. ORS 276A.346 is amended to read:

276A.346. (1) As used in this section:

(a) "Artificial intelligence" means a machine-based system that is capable, for a given set of human-defined objectives, of making predictions, recommendations or decisions influencing real or virtual environments and uses machine- or human-based inputs to:

(A) Perceive real or virtual environments;

(B) Abstract the perceptions into models through analysis in an automated manner; and

(C) Use model inference to formulate options for information or action.

[*(a)*] **(b)** "Covered product" means**:**

(A) Any form of hardware, software or service provided by a covered vendor.

(B) Any hardware, software or service that uses artificial intelligence and the artificial intelligence is developed or owned by a covered vendor.

[*(b)*] **(c)** "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)*] **(d)** "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 ORS 276A.344, 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 4. ORS 276A.348 is amended to read:

276A.348. (1) As used in this section:

(a) "Artificial intelligence" means a machine-based system that is capable, for a given set of human-defined objectives, of making predictions, recommendations or decisions influencing real or virtual environments and uses machine- or human-based inputs to:

(A) Perceive real or virtual environments;

(B) Abstract the perceptions into models through analysis in an automated manner; and

(C) Use model inference to formulate options for information or action.

[*(a)*] **(b)** "Covered product" means**:**

(A) Any form of hardware, software or service provided by a covered vendor.

(B) Any hardware, software or service that uses artificial intelligence and the artificial intelligence is developed or owned by a covered vendor.

[*(b)*] **(c)** "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)*] **(d)** "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 ORS 276A.344, 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.