ENTERPRISE information services

| DAS DEPARTMENT OF ADMINISTRATIVE SERVICES<br>STATEWIDE POLICY | **NUMBER**<br>107-004-155 | **SUPERSEDES**<br>~~New~~107-004-155<br>October 24, 2024 |
|---|---|---|
| | **EFFECTIVE DATE**<br>January 1, 2026<br>~~October 24, 2024~~ | **PAGE NUMBER**<br>Pages 1 of 4 |
| | **REVIEWED DATE** | |
| **DIVISION**<br>Enterprise Information Services | **REFERENCE**<br>• ORS Chapter ~~256~~396<br>• OAR 128-020-0005-0035<br>• Statewide Procedure 107-004-155_PR | |
| **POLICY OWNER**<br>Cyber Security Services | | |
| **SUBJECT**<br>Covered Products and Vendors | **APPROVED**<br>_____<br>Terrence Woods, State Chief Information Officer | |

## PURPOSE

This policy sets forth requirements for notice to state agencies that a corporate entity is designated or no longer designated a national security threat. Additionally, it provides schedules for implementing requirements regarding covered vendors and for incorporating the requirements into agency information security plans, standards or measures.

## APPLICABILITY

This policy applies to any board, commission, department, division, office, or other entity of state government, as defined in ORS 174.111, except the Secretary of State or State Treasurer.

## EXHIBITS

Attachment A: Covered Vendor/Product List and Template

## DEFINITIONS

**Agency IT leadership:** State agency Chief Information Officers, and state agency directors for those state agencies without a Chief Information Officer.

**Artificial Intelligence:** 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.

**Corporate entity:** Any type of organization or legal entity other than an individual natural person, such as a corporation, partnership, limited liability company, or other organization, whether incorporated or unincorporated.

**Covered product:** Any form of hardware, software or service provided by a covered vendor; and any hardware, software or service that uses artificial intelligence and the artificial intelligence is developed or owned by a covered vendor.

**Covered vendor:** Any of the following corporate entities, or any parent, subsidiary, affiliate or successor entity of the following corporate entities:

(1) Entities defined in Oregon Laws Chapter 256 Section 1(2)
(2) Any other corporate entity designated by the State Chief Information Officer as a covered vendor because it is a national security threat
(3) Any corporate entity that has been prohibited or had its products or services prohibited from use by a federal agency pursuant to the Secure and Trusted Communications Networks Act of 2019, 47 USC 1601, et seq, including as amended

**National security threat:** For purposes of protecting state information technology assets, a corporate entity that has been designated as a covered vendor because its covered product(s) pose(s) an unacceptable risk of harm to the operations of government, business entities, or the economy, or an unacceptable risk of harm to the rights and privacy of individuals, because of its engagement in a pattern or serious instance(s) of conduct significantly adverse to the security of federal or state infrastructure, government operations or systems, public and private institutions, law enforcement or military intelligence, individuals' personal information, or other sensitive or protected information.

**State agency:** 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.

**State information technology asset:** 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.

## EXCLUSIONS AND SPECIAL SITUATIONS

For investigatory, regulatory or law enforcement purposes, a state agency director must disclose justification to the Cyber Security Services assessment team via email* for:

(1) Installation or download of a covered product onto a state information technology asset
(2) Use or access of a covered product by a state information technology asset

A state agency that permits the installation, download, use or access of a covered product for investigatory, regulatory or law enforcement purposes will document and adopt risk mitigation standards and procedures related to the installation, download, use or access of the covered product.

* das_dl_oscio_css_risk_management_team@das.oregon.gov

## SCHEDULE FOR REVIEW

Covered products and vendors will be reviewed at least annually for determination by the State Chief Information Officer to add, retain or remove entities from the list.

## GENERAL INFORMATION

Subject to allowable investigatory, regulatory, or law enforcement exceptions, and all applicable policies and procedures, no covered products of a corporate entity listed as a covered vendor on the list maintained by the State Chief Information Officer may be installed or downloaded onto a state information technology asset that is managed or controlled by a state agency, or used or accessed by a state information technology asset. Covered products, covered vendors, and agency requirements within this policy will be included in regular assessments conducted by Cyber Security Services (CSS).

Failure to comply with this policy, including failure to implement requirements or provide sufficient justification of an investigatory or law enforcement need of a covered product, can result in immediate restriction and administrative action on the device(s), termination of connection to the state network and further communication to agency leadership for resolution.

(1) CSS will notify agency IT leadership when a corporate entity is designated or no longer designated a covered vendor. A current list of covered vendors with additional details is maintained on the publicly accessible EIS Covered Vendors page Enterprise Information Services: Covered Vendors.

(2) Upon designation of a corporate entity as a covered vendor by the State Chief Information Officer, state agencies implement the following requirements within 30 calendar days of notice:

A state agency will:

(a) Remove any covered product that is installed or downloaded onto a state information technology asset that the agency manages or controls; and

(b) Implement all measures necessary to prevent the:

- Installation or download of a covered product onto a state information technology asset that the agency manages or controls; and
- Use or access of a covered product by a state information technology asset that the agency manages or controls.

(3) Within 30 days after the effective date of this policy or notification of a change to covered vendors, agency IT leadership will notify the CSS assessment team that they have completed either:

(a) All actions required in item 2 of this policy, or

(b) Disclosure of justification by the agency director of an investigatory, regulatory or law enforcement need to use a covered product.

(4) State agencies will incorporate the requirements of item 2 of this policy into the agency's information security plans, standards or measures within 120 days of the effective date of this policy.

(5) State agencies using a covered product for investigatory, regulatory or law enforcement purpose, will report such usage and business justification to CSS on a quarterly basis.

## Attachment A: Covered Vendor/Product List Template

ENTERPRISE information services

### Covered Vendor List

### MMM DD, YYYY

In accordance with Oregon Administrative Rule 128-020, Oregon's State Chief Information Officer (CIO) maintains a Covered Vendor List.

Subject to allowable investigatory, regulatory, or law enforcement exceptions, and all applicable policies and procedures, no covered products of a corporate entity listed as a covered vendor on this list may be installed or downloaded onto a state information technology asset that is managed or controlled by a state agency, or used or accessed by a state information technology asset.

Please follow the current rule and policy for inclusion and full scope of this list and implementing requirements of this list.

## COVERED VENDOR LIST

(1) The following corporate entities:
- (a) Ant Group Co., Limited
- (b) ByteDance Limited (includes products such as TikTok)
- (c) Huawei Technologies Company Limited
- (d) Kaspersky Lab
- (e) Tencent Holdings Limited (includes products such as WeChat)
- (f) ZTE Corporation

(2) Corporate entities not already listed above that have been prohibited or had their products or services prohibited from use by a federal agency pursuant to the Secure and Trusted Communications Networks Act of 2019, 47 USC 1601, et seq, including as amended.

- (a) {List additional entities as presented by the FCC covered list at https://www.fcc.gov/supplychain/coveredlist}
- (b) {List additional entities designated by State Chief Information Officer}

_____ _____

Terrence Woods
State of Oregon Chief Information Officer

Date