OFFICE OF THE SECRETARY OF STATE
LAVONNE GRIFFIN-VALADE
SECRETARY OF STATE

CHERYL MYERS
DEPUTY SECRETARY OF STATE
AND TRIBAL LIAISON

ARCHIVES DIVISION
STEPHANIE CLARK
DIRECTOR

800 SUMMER STREET NE
SALEM, OR 97310
503-373-0701

PERMANENT ADMINISTRATIVE ORDER

FILED
01/29/2024 1:04 PM
ARCHIVES DIVISION
SECRETARY OF STATE
& LEGISLATIVE COUNSEL

OSCIO 1-2024
CHAPTER 128
DEPARTMENT OF ADMINISTRATIVE SERVICES
OFFICE OF THE STATE CHIEF INFORMATION OFFICER

FILING CAPTION: Adopting State Chief Information Officer rules to implement HB 3127 (2023) addressing Covered Vendor.

EFFECTIVE DATE: 02/01/2024

AGENCY APPROVED DATE: 01/25/2024

CONTACT: Shirlene Gonzalez
971-803-1766
shirlene.a.gonzalez@das.oregon.gov

550 Airport Road SE, STE C
Salem,OR 97301

Filed By:
Janet Chambers
Rules Coordinator

RULES:
128-020-0005, 128-020-0010, 128-020-0015, 128-020-0020, 128-020-0025, 128-020-0030, 128-020-0035

ADOPT: 128-020-0005

RULE TITLE: Purpose

NOTICE FILED DATE: 12/04/2023

RULE SUMMARY: Adopting to define purpose of rule for State Information Technology Asset Protection – Covered Vendors.

RULE TEXT:
(1) The State Chief Information Officer has responsibility for and authority over executive department information systems security in accordance with ORS 276A.300, including responsibility for taking all measures that are reasonably necessary to protect the availability, integrity or confidentiality of information systems or the information stored in information systems.
(2) The primary purpose of these rules is to establish the criteria and processes by which the State Chief Information Officer will determine when a corporate entity poses a national security threat, and when a corporate entity no longer poses a national security threat. These rules define “national security threat” for purposes of protecting state information technology assets.

STATUTORY/OTHER AUTHORITY: ORS 276A.300

STATUTES/OTHER IMPLEMENTED: Or Laws 2023, ch 256 (HB 3127)

ADOPT: 128-020-0010

RULE TITLE: Definitions

NOTICE FILED DATE: 12/04/2023

RULE SUMMARY: Adopting to define definitions.

RULE TEXT:

For the purposes of these Chapter 020 rules, the following definitions apply:

(1) “Corporate entity” means 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.

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

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

(a) The following corporate entities:

(A) Ant Group Co., Limited;

(B) ByteDance Limited;

(C) Huawei Technologies Company Limited;

(D) Kaspersky Lab;

(E) Tencent Holdings Limited; and

(F) ZTE Corporation.

(b) Any other corporate entity designated by the State Chief Information Officer as a covered vendor because it is a national security threat.

(c) 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.

(4) “National security threat” means, 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.

(5) “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.

(6) “State information technology asset” means any form of hardware, software or service for data processing, office automation, or telecommunications that is 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.

STATUTORY/OTHER AUTHORITY: ORS 276A.300

STATUTES/OTHER IMPLEMENTED: Or Laws 2023, ch 256 (HB 3127)

ADOPT: 128-020-0015

RULE TITLE: Covered Vendor List

NOTICE FILED DATE: 12/04/2023

RULE SUMMARY: Adopting to describe Covered Vendor list to be established and maintained by the State Chief Information Officer.

RULE TEXT:

(1) The State Chief Information Officer shall establish a list of covered vendors on its publicly accessible website, inclusive of information sufficient to identify covered products, and the date that each covered vendor was designated as a national security threat. The State Chief Information Officer shall maintain and update this list in accordance with the policies and procedures adopted pursuant to OAR 128-020-0025, Designation Process.

(2) 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 under this Division 20 may be installed or downloaded onto a state information technology asset that is under the management or control of a state agency, or used or accessed by a state information technology asset.

STATUTORY/OTHER AUTHORITY: ORS 276A.300

STATUTES/OTHER IMPLEMENTED: Or Laws 2023, ch 256 (HB 3127)

ADOPT: 128-020-0020

RULE TITLE: Designation Criteria

NOTICE FILED DATE: 12/04/2023

RULE SUMMARY: Adopting to describe the criteria the State Chief Information Officer will consider when designating a Covered Vendor.

RULE TEXT:

The State Chief Information Officer will consider one or more of the following criteria when determining if a corporate entity is a national security threat:

(1) The corporate entity owns or otherwise provides a product or service that was developed or provided by a covered vendor.

(2) The extent to which the corporate entity is affiliated with a covered vendor.

(3) The corporate entity owns or otherwise provides a product or service that collects user data, including but not limited to personal information, browsing history, and location history, that is not required for or grossly exceeds the minimum necessary user data for the product or service.

(4) The corporate entity owns or otherwise provides a product or service that collects user data, such as biometric data, contact information, GPS locations, chat logs, photos and browser histories, personal information, browsing history, and location history, that is potentially or currently accessible by foreign governments or foreign state actors.

(5) The corporate entity owns or otherwise provides a product or service that has security vulnerabilities that, if unresolved, could expose state information technology assets to malicious actors.

(6) The corporate entity owns or otherwise provides a product or service developed or provided by a corporate entity that has been designated a national security threat or otherwise meets the criteria of a covered vendor under OAR 128-020-0010.

(7) The corporate entity owns or otherwise provides a product or service that supports the administrative use of algorithmic modifications to conduct misinformation, disinformation, or malinformation campaigns.

(8) The corporate entity owns or otherwise provides a product or service that has the potential to control or compromise state information technology assets.

STATUTORY/OTHER AUTHORITY: ORS 276A.300

STATUTES/OTHER IMPLEMENTED: Or Laws 2023, ch 256 (HB 3127)

ADOPT: 128-020-0025

RULE TITLE: Designation Process

NOTICE FILED DATE: 12/04/2023

RULE SUMMARY: Adopting to reference policy and procedure for designation process and schedule.

RULE TEXT:

(1) Enterprise Information Services shall adopt and implement a policy and procedure that establishes the schedule for review of corporate entities associated with hardware, software, and services against the criteria in OAR 128-020-0020, and under which Enterprise Information Services will update its covered vendor list to reflect designations made pursuant to the Secure and Trusted Communications Networks Act of 2019, 47 USC 1601, et seq, including as amended. If review or other update identifies that a corporate entity is or may be a national security threat, the State Chief Information Officer will determine if the corporate entity should be designated as a covered vendor.

(2) The determination of the State Chief Information Officer will be reflected in an update of the covered vendor list on the publicly accessible Enterprise Information Services website.

STATUTORY/OTHER AUTHORITY: ORS 276A.300

STATUTES/OTHER IMPLEMENTED: Or Laws 2023, ch 256 (HB 3127)

ADOPT: 128-020-0030

RULE TITLE: De-Designation Criteria

NOTICE FILED DATE: 12/04/2023

RULE SUMMARY: Adopting to describe the criteria the State Chief Information Officer will consider when de-designating a Covered Vendor.

RULE TEXT:
The State Chief Information Officer will consider one or more of the designation criteria in OAR 128-020-0020 when de-designating or re-evaluating a corporate entity's status as a national security threat.

STATUTORY/OTHER AUTHORITY: ORS 276A.300

STATUTES/OTHER IMPLEMENTED: Or Laws 2023, ch 256 (HB 3127)

ADOPT: 128-020-0035

RULE TITLE: De-Designation Process

NOTICE FILED DATE: 12/04/2023

RULE SUMMARY: Adopting to describe the process of de-designation of a Covered Vendor.

RULE TEXT:

(1) If review or other update received pursuant to the process and procedure established under OAR 128-020-0025, Designation Process, identifies that a corporate entity may no longer pose a national security threat, the State Chief Information Officer will determine if the corporate entity should be removed from the covered vendor list.

(2) The determination of the State Chief Information Officer will be reflected in an update of the covered vendor list on the publicly accessible Enterprise Information Services website.

STATUTORY/OTHER AUTHORITY: ORS 276A.300

STATUTES/OTHER IMPLEMENTED: Or Laws 2023, ch 256 (HB 3127)