Covered Vendors

Ben Gherezgiher
State Chief Information Security Officer

Terrence Woods
State Chief Information Officer

Joint Committee on Information Management and Technology

March 14, 2025

ENTERPRISE information services

Agenda

- House Bill 3127
- Oregon Administrative Rules 128-020
- Policy Exclusions and Timeframes
- Current Covered Vendor List
- DeepSeek

ENTERPRISE information services

House Bill 3127 (2023)

- Definitions
- Initial list of Covered Vendors
- Directed State CIO to write rules and policy
  - Oregon Administrative Rules
  - Covered Products and Vendors Statewide Policy
  - Covered Products and Vendors Statewide Procedure
  - Statewide Covered Vendor List

Definitions

- **Covered product:** any form of hardware, software or service provided by a covered vendor.
- **Covered vendor:**
  - entities defined in law
  - entities designated by the State Chief Information Officer as a national security threat
  - entities prohibited by a federal agency pursuant to the Secure and Trusted Communications Networks Act of 2019, 47 USC 1601, et seq, including as amended
- **State agency:** any board, commission, department, division, office, or other entity of state government, as defined in ORS 174.111, except Secretary of State or State Treasurer

Definitions

- **National security threat:** 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

Initial list of Covered Vendors in statute

- Ant Group Co., Limited
- ByteDance Limited
- Huawei Technologies Company Limited
- Kaspersky Lab. (e) Tencent Holdings Limited
- ZTE Corporation

Oregon Administrative Rules – Covered Vendors

- 128-020-0005: Purpose
- 128-020-0010: Definitions
- 128-020-0015: Covered Vendor List
- 128-020-0020: Designation Criteria
- 128-020-0025: Designation Process
- 128-020-0030: De-Designation Criteria
- 128-020-0035: De-Designation Process

Exclusion 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
- Agency must document and adopt risk mitigation standards and procedures related to the installation, download, use or access of the covered product

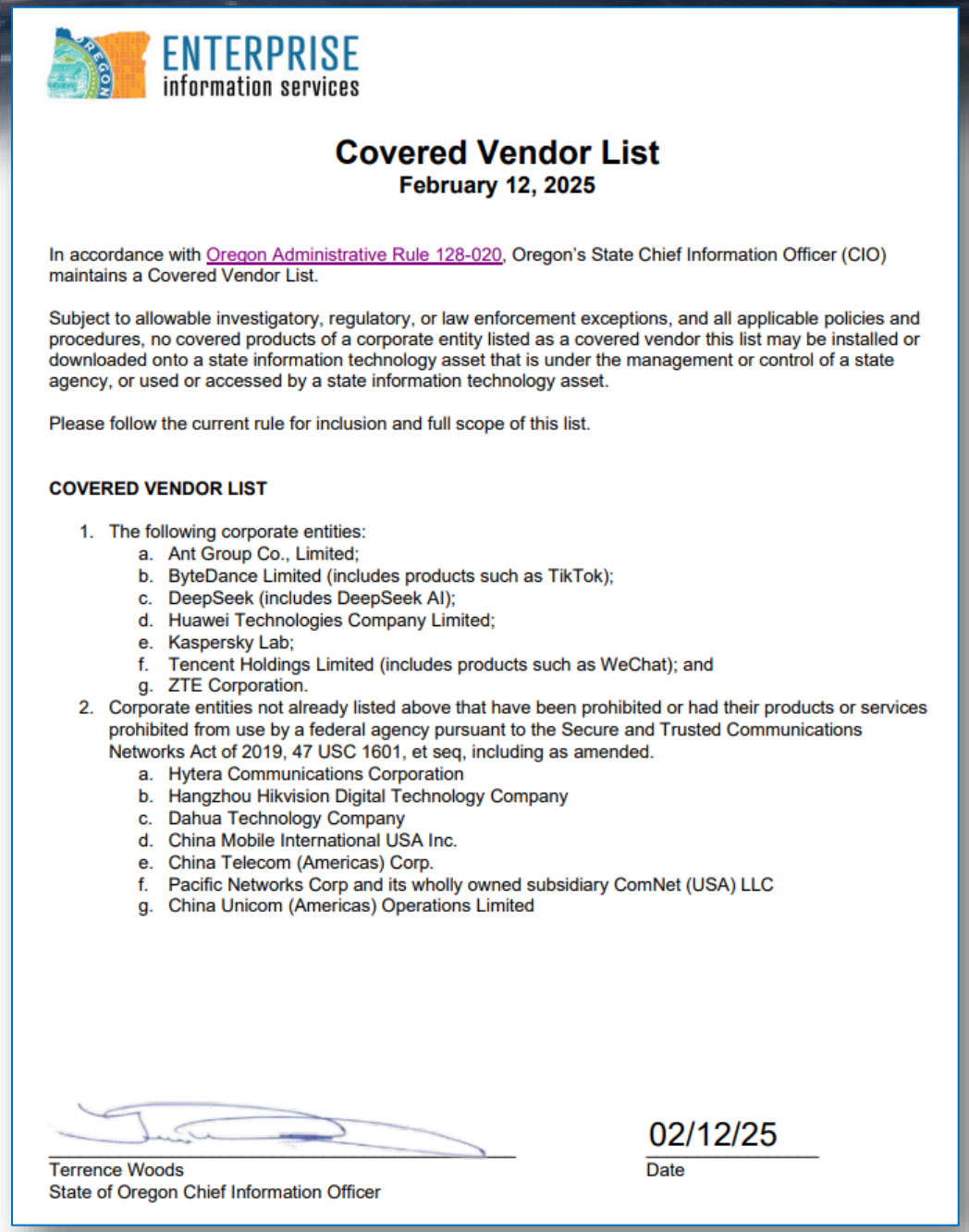
Policy Timeframes

- Within 30 calendar days of notice, a state agency will:
  - Remove any covered product
  - Implement all measures necessary to prevent the:
    - Installation or download of a covered product
    - Use or access of a covered product
  - Notice Cyber Security Services of their status of compliance
- Quarterly, state agencies using a covered product for investigatory, regulatory or law enforcement purpose, will report such usage and business justification to Cyber Security Services

ENTERPRISE information services

Covered Vendor List

- The list and related law and policy framework is maintained to provide an additional layer of security to protect the state's critical information assets
- The government sponsored bad actors are known to embed malware that can result in unauthorized data leaks that can be used to develop potential cyber threats



ENTERPRISE information services

Covered Vendor List
February 12, 2025

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 this list 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.

Please follow the current rule for inclusion and full scope 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. DeepSeek (includes DeepSeek AI);
   d. Huawei Technologies Company Limited;
   e. Kaspersky Lab;
   f. Tencent Holdings Limited (includes products such as WeChat); and
   g. 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. Hytera Communications Corporation
   b. Hangzhou Hikvision Digital Technology Company
   c. Dahua Technology Company
   d. China Mobile International USA Inc.
   e. China Telecom (Americas) Corp.
   f. Pacific Networks Corp and its wholly owned subsidiary ComNet (USA) LLC
   g. China Unicom (Americas) Operations Limited

Terrence Woods
State of Oregon Chief Information Officer

02/12/25
Date

DeepSeek

- Poses significant risk to collected data such as:
  - Censorship and information control
  - Data privacy and security concerns
  - Personally Identifiable Information risk
  - Usage (data) information
- All data collected by DeepSeek AI is stored on services hosted in the People's Republic of China
- Data processed by DeepSeek AI is accessible to the Chinese government
- Unsecured databases containing highly sensitive information, posing a significant risk of exploitation by threat actors


ENTERPRISE
information services
Thank you
Shirlene Gonzalez
Legislative Director
shirlene.a.gonzalez@das.oregon.gov