Maryland

DEPARTMENT OF INFORMATION TECHNOLOGY

Office of Security Management

DIRECTIVE 2022-12-001 (UPDATED)

Prohibited Technologies Policy

Version 1.1
Date Issued: December 6, 2022
Date Last Revised: December 13, 2024

Table of Contents

Revision Control History

Version	Author(s)	Date	Description
1.0	Greg Rogers	December 6, 2022	Initial Version
1.1	Greg Rogers	October 11, 2024	Updated to remove company from list
1.1	Greg Rogers	December 13, 2024	Final Version Completed

Approval

Gregory S Rogers 12/13/2024

Gregory S Rogers — Date
State Chief Information Security Officer

Background

The Office of Security Management (OSM) is responsible for establishing security requirements for information and information systems (Md. Code, State Fin. & Proc. ("SF&P") § 3.5-2A-04), and is headed by the State Chief Information Security Officer (State CISO) (SF&P § 3.5-2A-03).

Certain vendors and products present an unacceptable level of cybersecurity risk to the State, including products where the State has a reasonable belief that the manufacturer or vendor may participate in activities such as:

- Inappropriate collection of sensitive personal information
- Cyber-espionage
- algorithmic modification to conduct disinformation or misinformation campaigns
- surveillance of government entities

Pursuant to SF&P § 3.5-2A-04, if the State CISO determines that there are security vulnerabilities or deficiencies in any information systems, the State CISO may determine and direct or take actions necessary to correct or remediate the vulnerabilities or deficiencies, which may include requiring the information system to be disconnected.

Scope

This directive applies to all in the Maryland State government's executive branch. Entities not included in the scope should strongly consider complying with this directive.

Except where approved exceptions apply, the use or installation of products and services covered by this Directive is prohibited on all government-owned or -leased devices, including but not limited to cell phones, tablets, desktop and laptop computers, servers, Internet-of-Things (IOT) devices, Operational Technology (OT), Industrial Control Systems (ICS) and other internet-capable devices.

This Directive will also apply to personal devices used to connect to State systems, or otherwise conduct State business.

Products Subject to this Directive

The following vendors and products, along with the date added, are subject to this directive.

December 6, 2022 (update October 11, 2024) – State Prohibitions

- Tencent Holdings, including but not limited to:
  - Tencent QQ
  - QQ Wallet
  - WeChat
- AliPay
- TikTok

Updated October 11, 2024 – Federal Prohibitions

Covered Equipment or Services*	**Date of Inclusion on Covered List**
Telecommunications equipment produced by **Huawei Technologies Company**, including telecommunications or video surveillance services provided by such entity or using such equipment.	March 12, 2021
Telecommunications equipment produced by **ZTE Corporation**, including telecommunications or video surveillance services provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced by **Hytera Communications Corporation**, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced by **Hangzhou Hikvision Digital Technology Company**, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services provided by such entity or using such equipment.	March 12, 2021
Video surveillance and telecommunications equipment produced	March 12, 2021

Covered Equipment or Services*	Date of Inclusion on Covered List
by **Dahua Technology Company**, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services provided by such entity or using such equipment.	
Information security products, solutions, and services supplied, directly or indirectly, by **AO Kaspersky Lab** or any of its predecessors, successors, parents, subsidiaries, or affiliates.	March 25, 2022
International telecommunications services provided by **China Mobile International USA Inc**. subject to section 214 of the Communications Act of 1934.	March 25, 2022
Telecommunications services provided by **China Telecom (Americas) Corp.** subject to section 214 of the Communications Act of 1934.	March 25, 2022
International telecommunications services provided by **Pacific Networks Corp** and its wholly owned subsidiary **ComNet (USA) LLC** subject to section 214 of the Communications Act of 1934.	September 20, 2022
International telecommunications services provided by **China Unicom (Americas) Operations Limited** subject to section 214 of the Communications Act of 1934.	September 20, 2022
Cybersecurity and anti-virus software produced or provided by **Kaspersky Lab, Inc.** or any of its successors and assignees, including equipment with integrated Kaspersky Lab, Inc. (or any of its successors and assignees) cybersecurity or anti-virus software.	July 23, 2024

* The Covered List is sourced from **Federal Communications Commission** regulation *47 U.S.C. §§ 1601–1609 (2020)* Section 2 Covered List https://www.fcc.gov/supplychain/coveredlist

Required Actions

In-Scope Units of State Government

Within fourteen days of issuance or modification of this document, units must:

1. Remove any referenced hardware and/or software products from State-owned or managed technology assets under their control, and
2. Implement measures to prevent the installation of referenced hardware and software products on State-owned or managed technology assets, and
3. Implement network-based restrictions to prevent the use of, or access to, prohibited services.
    . Because networkMaryland™ provides Internet services to organizations outside the scope of this directive, this traffic will not be blocked by networkMaryland™

Implementation Guidance

Use-Case Specific Guidance

Hardware Products

a. No specific guidance for this use case is available at this time.

Desktop Applications

b. Units should use automated tools, where possible, to remove prohibited applications.
c. Administrative permissions should be restricted to those with a business purpose.

Mobile Applications

d. Units should implement mobile device management software to ensure they have an up- to-date inventory of applications installed on mobile devices.
e. Units should restrict access to State data and applications (e.g., Google Mail) on mobile devices to only those managed by the State and explicitly authorized to have access.

Networks and Firewalls

f. Units should implement application-aware rules to restrict access to prohibited applications.
g. Units should implement detective measures to identify State-owned assets that have or attempt to access prohibited applications.

Exceptions

Requests for exceptions and extensions must be submitted to the Office of Security Management by emailing the GRC Team at doit.grc@maryland.gov.