Maryland

DEPARTMENT OF
INFORMATION TECHNOLOGY

Office of Security Management

EMERGENCY DIRECTIVE 2022-12-001

Remove Prohibited Products and Platforms

Table of Contents

Revision History

Version	Date	Description of Changes
1.0.0	December 6, 2022	Initial Version

Approval

Charles I Stewart III

Charles "Chip" Stewart
State Chief Information Security Officer

12/6/2022
Date

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

Products Subject to this Directive

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

December 6, 2022

- Huawei Technologies
- ZTE Corp
- Tencent Holdings, including but not limited to:
  - Tencent QQ
  - QQ Wallet
  - WeChat
- Alibaba products, including but not limited to:
  - AliPay
- Kaspersky
- TikTok

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 products from the state networks, and
2. Remove any referenced software products from the state networks, and
3. Implement measures to prevent the installation of referenced hardware and software products on State-owned or managed technology assets, and
4. Implement network-based restrictions to prevent the use of, or access to, prohibited services[1,2].

Office Of Security Management

- Take action pursuant to SF&P § 3.5-2A-04, as directed by the State Chief Information Security Officer, to mitigate a threat created by a referenced product or vendor.

[1] For Managed Firewall Customers, the Office of Security Management will follow established change-management and communication processes to implement firewall rules consistent with the referenced requirements.
[2] 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

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

Desktop Applications

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

Mobile Applications

- Units should implement mobile device management software to ensure they have an up-to-date inventory of applications installed on mobile devices.
- 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

- Units should implement application-aware rules to restrict access to prohibited applications.
- 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 Security Operation Center at soc@maryland.gov.