JOINT CIRCULAR

STATE OF NEW JERSEY
OFFICE OF HOMELAND SECURITY AND PREPAREDNESS

NO.: 23-01-NJCCIC/OIT/DPP	ORIGINATING AGENCY: OFFICE OF HOMELAND SECURITY AND PREPAREDNESS (OHSP) NEW JERSEY CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL (NJCCIC) OFFICE OF INFORMATION TECHNOLOGY (OIT) OFFICE OF MANAGEMENT AND BUDGET (OMB) DIVISION OF PURCHASE AND PROPERTY (DPP)	PAGE 1 OF 3
EFFECTIVE DATE: 01/09/2023		EXPIRATION DATE: INDEFINITE

SUBJECT: PROHIBITED AND HIGH RISK SOFTWARE ON STATE PROVIDED OR MANAGED DEVICES

ATTENTION: DIRECTORS OF ADMINISTRATION, CHIEF FISCAL OFFICERS, CHIEF INFORMATION OFFICERS, AGENCY INFORMATION TECHNOLOGY MANAGERS, AGENCY INFORMATION SECURITY OFFICERS, AGENCY PROCUREMENT MANAGERS, AND AGENCY SECURITY MANAGERS

FOR INFORMATION CONTACT:

NJCCIC GOVERNANCE, RISK, AND COMPLIANCE BUREAU	riskreview@cyber.nj.gov
OIT IT PROCUREMENTS	OIT.oitprocure-req@tech.nj.gov
OMB NON-IT PROCUREMENTS	equipment@sp3.treas.state.nj.us

I. Purpose

The purpose of this Circular is to help ensure the confidentiality, integrity, availability, privacy, and safety of New Jersey state government - provided or managed information assets through the implementation of controls that prohibit the acquisition, installation, and use of software products and services that present an unacceptable level of cybersecurity risk to the State.

II. Scope and Applicability

This Circular applies to all Departments, Agencies, Commissions, Boards, Bodies, or other instrumentalities of the Executive Branch of New Jersey State Government, hereinafter referred to as: Agencies, the Executive Branch, or the State.

All Executive Branch full-time and part-time employees, temporary workers, volunteers, interns, contractors, and those employed by contracted entities – collectively referred to as users - are governed by and responsible for complying with this Circular regardless of agency, location, or role.

III. Policy

The New Jersey Cybersecurity and Communications Integration Cell (NJCCIC), in collaboration with the Office of Information Technology (OIT)), shall establish a list of technology vendors and software products and services that present an unacceptable level of cybersecurity risk to the State.

IV. Prohibited Software Vendors, Products, and Services as of January 9, 2023:

1. Huawei Technologies
2. Zhejiang Dahua Technology Co., Ltd., also doing business as Dahua
3. Hangzhou Hikvision Digital Technology Co., Ltd., also doing business as Hikvision
4. Tencent Holdings LTD, including but not limited to:
    a. WeChat
    b. QQ
    c. QQ Wallet
5. Alibaba products, including but not limited to:
    a. AliPay
    b. Alibaba.com Mobile Apps
6. Hytera
7. ZTE Corporation
8. ByteDance Ltd., including but not limited to TikTok
9. Kaspersky Lab

The NJCCIC and OIT will continually monitor and update the Prohibited Software and Services Vendors and Products list. The updated list will be posted to the NJCCIC website, cyber.nj.gov.

V. Required Actions:

Agencies shall, as applicable:

A. Remove any referenced software products from State-owned, provided, or managed systems and devices;

B. Implement network-based restrictions to prevent the use of, or access to, prohibited software or services;

C. Implement measures to prevent the installation of referenced high-risk software products on State-owned or managed technology assets; and

D. Develop and implement plans to include risks associated with of referenced high-risk software products and supply chain security into cybersecurity awareness and training programs.

VI. Exceptions:

Agencies may have public health, safety, welfare, or other compelling State business and public interest reasons for using the above prohibited software technologies or services. In such cases, the Agencies are required to submit an exception request with the NJCCIC at riskreview@cyber.nj.gov. Approved exceptions and use cases will include risk mitigation instructions.

VII. Supplemental Guidance:

Beyond the list of prohibited software vendors and products, Agencies should review supplier risks in all IT procurements and uses, including but not limited to: foreign ownership, control or

influence (FOCI), and the ability of the supplier to effectively assess subordinate second-tier and third-tier suppliers and contractors.

Agencies should review the US Department of Commerce Bureau of Industry and Security Lists of Parties of Concern, the International Trade Association Consolidated Screening List, and the National Defense Authorization Act (NDAA) Section 889 prior to contracting with a supplier.

Further Software and Supply Chain Security policies, standards, and guidance can be found in the Statewide Information Security Manual (SISM). This Circular shall be included as an addendum to the SISM. Agencies should contact the NJCCIC for further guidance.