Joe Lombardo
Governor

Jack Robb
Director

Matthew Tuma
Deputy Director

Timothy D. Galluzi
Administrator/State CIO

Darla J. Dodge
Deputy Administrator

STATE OF NEVADA
DEPARTMENT OF ADMINISTRATION
Enterprise IT Services Division
100 N. Stewart Street, Suite 100 | Carson City, Nevada 89701
Phone: (775) 684-5800 | www.it.nv.gov | eitsadministration@admin.nv.gov | Fax: (775) 687-9097

March 6, 2023

TO: All Agencies

FROM: Timothy D. Galluzi, EITS Administrator and State CIO

SUBJECT: New State Security Standard: System, Application, and Service Blacklisting

The State Information Security Committee (SISC), established via NRS 242.101, 242.111, and 242.115, comprised of information security and information technology leaders from across the executive branch, have established standard S.6.02.07 - System, Application, and Service Blacklisting. This new standard creates a process in which applications, hardware, or software that pose a significant security risk to the State of Nevada's infrastructure and data, may be blacklisted, and prohibited on state-owned devices, networks, and platforms.

The State's Chief Information Security Officer, Bob Dehnhardt, and I have signed this standard, which became effective January 26, 2023.

Enterprise IT Services Division's Office of Information Security will maintain a list of items that have been added to the State Blacklist. An agency's SISC representative may recommend additions or modifications to the State Blacklist through the SISC. Agencies may maintain internal blacklists that are more stringent than the State Blacklist but not more lenient.

If any agency requires an exemption, the process for requesting consideration can be initiated via S.2.04.01.1F – State Security PSP Exemption Request found here:
https://it.nv.gov/Governance/Security/State_Security_Policies_Standards___Procedures/

While implementing the standard, the SISC adopted the inaugural list of items to be included in the State Blacklist. Those products include:

- Alibaba products, including but not limited to AliPay*
- China Mobile International USA Inc.*
- China Telecom (Americas) Corp.*
- China Unicom (Americas) Operations Limited*
- Dahua Technology Company*
- Grammarly

- Hangzhou Hikvision Digital Technology Company*
- Huawei Technologies*
- Hytera Communications Corporation*
- Kaspersky*
- Pacific Network Corp/ComNet (USA) LLC*
- Tencent Holdings, including but not limited to Tencent QQ, QQ Wallet, and WeChat*
- TikTok
- ZTE Corporation*

*Added due to federal ban

I would like to thank the dedicated information security professionals and agency representatives who serve on the SISC not only for the work that was done in creation of this standard, but for the work that they do every day to secure our critical technology infrastructure and data.

Questions regarding this standard can be sent to the Office of Information Security (infosec@admin.nv.gov) or to my office (EITSAdministration@admin.nv.gov). A copy of Standard S.6.02.07 and the inaugural list are enclosed.

Enclosures: Standard S.6.02.07 - System, Application, and Service Blacklisting
Standard S.6.02.07A - Blacklist