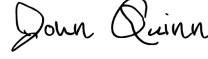


TO: All Executive Branch Agencies, Departments, and Offices

FROM: John Quinn, Secretary, Agency of Digital Service

DocuSigned by:

4333BDE6B4F74AB...

DATE: June 13, 2022

SUBJECT: Cybersecurity Standard Update 2022-01

This Cybersecurity Standard revises and supersedes Cybersecurity Standard Update 19-01 (February 19, 2019).

References:

- a) 3 V.S.A. § 2283(b)
- b) 3 V.S.A. § 2222(a)
- c) Department of Homeland Security Binding Operational Directive 01-17
- d) John S. McCain National Defense Authorization Act for Fiscal Year 2019
- e) 2019 Worldwide Threat Assessment of the US Intelligence Community
- f) United States [Public Law 115-232](#), section 889

Cybersecurity Standards issued by the Agency of Digital Services (ADS) are direction to all executive branch State Agencies pursuant to References (a) and (b) for the purposes of safeguarding State of Vermont information and information systems. "State Agency" as used in this Standard shall include all State agencies, departments, commissions, committees, authorities, divisions, boards or other administrative units of the Executive Branch.

Background:

The ever-evolving nature of cyber threats has continued to prove that the State of Vermont and the valuable data that we hold for our citizens is a priority target for cyber criminals and hackers alike. The Agency of Digital Services (ADS) has determined that the risks presented by Kaspersky-branded products or services, and covered telecommunications equipment or services including those provided by Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company justify issuance of this Cybersecurity Directive.

The federal cybersecurity and intelligence communities have documented evidence of the concerns regarding these products or telecommunications equipment and have used several mechanisms, including References (c), (d), (e) and (f) to block their use within the federal technology community. These concerns include:

- A. The broad access to files and elevated privileges of anti-virus software, including Kaspersky software; ties between Kaspersky officials and Russian government agencies; and requirements under Russian law that allow Russian intelligence agencies to request or

compel assistance from Kaspersky and to intercept communications transiting between Kaspersky operations in Russia and Kaspersky customers, including government customers in the United States.

- B. The US Intelligence Communities' assessment, cited in Reference (e), expressing concern "about the potential for Chinese intelligence and security services to use Chinese information technology firms as routine and systemic espionage platforms against the United States and allies."

Therefore:

1. The acquisition or renewal of any contract or grant, or use for a new purpose of Kaspersky-branded products on all State of Vermont information systems, or any vendor system, is prohibited.
 - a. "Kaspersky-branded products" means information security products, solutions, and services supplied, directly or indirectly, by AO Kaspersky Lab or any of its predecessors, successors, parents, subsidiaries, or affiliates, including Kaspersky Lab North America, Kaspersky Lab, Inc., and Kaspersky Government Security Solutions, Inc. (collectively, "Kaspersky"), including those identified below.
 - b. Kaspersky-branded products currently known to ADS are: Kaspersky Anti-Virus; Kaspersky Internet Security; Kaspersky Total Security; Kaspersky Small Office Security; Kaspersky Anti Targeted Attack; Kaspersky Endpoint Security; Kaspersky Cloud Security (Enterprise); Kaspersky Cybersecurity Services; Kaspersky Private Security Network; and Kaspersky Embedded Systems Security.
2. The acquisition or renewal of any contract or grant, or use for a new purpose of equipment manufactured by the companies listed in paragraph 2.a that is supporting any State of Vermont information systems, or any vendor system, is prohibited.
 - a. Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company. This includes equipment used to support any information technology, telecommunications, industrial control system, supervisory control and data acquisition system, systems used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other security purposes, building infrastructure support, or video surveillance purpose.
3. The acquisition or renewal of any contract or grant, or use for a new purpose of equipment manufactured by any telecommunications, or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense has identified as an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country as provided under United States Public Law 115-232.

4. Any request for exception to this Standard will be considered on a case-by-case basis, submitted with a plan of action with milestones for transition away from the prohibited items, by the Secretary of Digital Services after receiving a request, endorsed by the Secretary of the requesting State Agency and the Chief Information Security Officer, articulating the compelling justification for additional time to implement the requirements.
5. Nothing in this standard shall be construed to endorse or permit any current use of these technologies.
6. Internal point of contact for this Directive is Scott Carbee, State of Vermont Chief Information Security Officer, at Scott.Carbee@Vermont.gov .