Department of MANAGEMENT SERVICES
We Serve Those Who Serve Florida

4050 Esplanade Way
Tallahassee, FL 32399-0950
850-488-2786

Ron DeSantis, Governor
Pedro Allende, Secretary

MEMORANDUM

TO: State Agency Head or Government Chief Executive Addressed

FROM: Pedro Allende, Secretary
Florida Department of Management Services

SUBJECT: Protect Floridians' Data from Foreign Countries of Concern

DATE: February 15, 2023

Florida's state and local governments face constant cyber threats that have the potential to harm Floridians, including from foreign adversaries who seek to sabotage and corrupt key information software and systems and steal intellectual property, information or critical infrastructure, and personal information.

Recognizing this growing threat, on September 22, 2022, Governor DeSantis signed Executive Order 22-216 (Strengthening Florida Cyber Security Against Foreign Adversaries) which directed the Department of Management Services (DMS) to *promulgate rules and take any additional action necessary… to ensure commodities and services used by state and local governments are not susceptible to exploitation by foreign countries of concern as defined in section 286.101, Florida Statutes (F.S.).*

DMS, through the Florida Digital Service (FL[DS]), as the lead entity responsible for modernizing state technology and information services and for determining appropriate cybersecurity measures for state agencies and through directives of Executive Order 22-216, has identified applications, software, websites, and other systems associated with QQ, TikTok, WeChat, VKontakte, and Kaspersky as posing a risk of unauthorized access to the data, including data of Floridians housed on state assets.

Accordingly, DMS is recommending state agencies implement managerial, operational, and technical safeguards to remove, block, an prevent all forms of access to all state agency networks, devices or other assets of the entities identified above. Specifically, state agencies should remove such access from:

- Device-management portals used by state employees to download applications to devices;
- Government-issued mobile devices, including tablets and phones;
- Government-issued computers; and
- All devices connecting to the internet via government provided networks, including guest networks

DMS also strongly recommends that local governments implement these safeguards and offers any assistance necessary to ensure the digital assets of all government entities are made secure.

DMS, through FL[DS], will further coordinate with state agency Inspectors General, Chief Information Officers, and Information Security Managers to identify additional specifications and to assist in the implementation of these safeguards.

Additionally, the DMS Division of Telecommunications in coordination with the Cybersecurity Operations Center, will identify network traffic across the enterprise and work to prevent connections to services, servers, and IP ranges of concern. In support of this effort, DMS requests state agencies communicate these recommendations with contracted external service providers and work to ensure they adhere to state agency security policies (see Rule 60GG-2.002(1)(d)6., Florida Administrative Code). DMS will continue to ensure contractual terms and conditions for enterprise contracts are compliant with security policies.

We look forward to continuing to discuss these emerging threats through the Enterprise Leaders Meetings and cybersecurity working groups. The Cybersecurity Operations Center will continue to hunt for digital threats to the state of Florida and will periodically provide additional recommendations.

DMS stands ready to assist your agencies in implementation of these important cybersecurity measures to protect from threats of foreign countries of concern.

Pedro Allende, Secretary