



OFFICE OF THE GOVERNOR

EXECUTIVE ORDER #184

Relating to Cybersecurity and Prohibiting the Use of Certain Foreign Technologies

WHEREAS, preserving the safety, security, privacy, and way of life of the people of Wisconsin is of paramount importance, and the State has gained information and recommendations regarding growing threats imposed by certain foreign vendors, products, and technologies that could pose cybersecurity threats, as well as digital privacy and other state and national security risks, which are contrary to the interests of the State and the people of Wisconsin;

WHEREAS, one of those products, TikTok, is a video-sharing mobile application with more than 94 million users in the United States as of 2022, and is owned by a ByteDance Ltd., which has a subsidiary that is partially owned by the Chinese Communist Party;

WHEREAS, TikTok can purportedly harvest large amounts of data from devices it is installed on, including when, where, and how the user conducts Internet activity;

WHEREAS, under China's 2017 National Intelligence Law, all businesses registered or that have operations in China are required to assist the government of China in intelligence work, including data sharing and data collecting, which, according to the Federal Bureau of Investigation, poses national security concerns that could compromise personal and government data and security;

WHEREAS, there are foreign actors alike that produce telecommunications and video/audio equipment, as well as other technologies and platforms, and we reasonably believe that use of these products may enable the manufacturer or vendor to:

- Collect sensitive personal, financial, proprietary, intellectual property, or other business data;
- Enable certain digital technologies, including email, to be compromised and act as a vector for ransomware deployment;
- Conduct cyber-espionage against government and other entities;
- Conduct surveillance and tracking of individual users; and
- Use algorithmic modifications to conduct disinformation or misinformation campaigns;

WHEREAS, the Wisconsin Department of Administration (DOA) Division of Enterprise Technology (DET) (hereinafter referred to jointly, where applicable, as "DOA-DET"), pursuant to Sections 16.971 through 16.975 of the Wisconsin Statutes is responsible for establishing, and has already established, security requirements and safeguards for State information and information systems, and is led by the State Chief Information Officer (State CIO) and State Chief Information Security Officer (State CISO) who continually monitor cybersecurity and implement all feasible technical means to ensure the security of all State information and information systems; and

WHEREAS, recognizing that, in the digital age, maintaining cybersecurity is critical to state and national security and that new and emerging technologies and applications could pose future potential safety, security, and privacy risks, the State of Wisconsin reaffirms its commitment to regular, ongoing review of such technologies to protect the interests of the State and of the people of Wisconsin.

NOW, THEREFORE, I, TONY EVERS, Governor of the State of Wisconsin, pursuant to the authority vested in me by the Constitution and the Laws of this State hereby order, effective immediately, that:

- 1) To best preserve the safety, security, and privacy of the people of Wisconsin, DOA-DET, consistent with its statutory mandates and in accordance with its existing policies, procedures, and processes, which include but are not limited to cybersecurity plans, will continue to use information gathered through state, federal, and industry-led intelligence to investigate vulnerabilities presented by products from foreign vendors, including when foreign companies may use Americans' user information for sensitive intelligence gathering, intellectual property theft, and other illicit purposes, and where there may be a reasonable belief that the manufacturer or vendor may participate in activities such as but not limited to:
 - a. Collecting sensitive citizen, financial, proprietary, intellectual property, or other business data;
 - b. Enabling email compromise and acting as a vector for ransomware deployment;
 - c. Conducting cyber-espionage against government entities;
 - d. Conducting surveillance and tracking of individual users; and
 - e. Using algorithmic modifications to conduct disinformation or misinformation campaigns.

- 2) DOA-DET, in collaboration with the Governor, the Office of the Governor, and state, federal, and industry-led intelligence, will continue to use such information to evaluate and identify applications and vendors that, due to the risk presented to state information or state information systems, may not be used in or connected to any State network or installed on any State-issued device, including but not limited to desktop computers, laptops, tablets, cellular phones, and other mobile devices. The State CISO shall communicate any identified prohibited foreign products to the Wisconsin Information Sharing and Analysis Committee (WI ISAC) and Agency IT Directors, per DET's normal communications processes. As of the date of this Order, the following vendors and/or software are prohibited from being utilized:
 - TikTok
 - Huawei Technologies
 - ZTE Corp
 - Hytera Communications Corporation
 - Hangzhou Hikvision Digital Technology Company
 - Dashua Technology Company
 - Tencent Holdings, including but not limited to:
 - Tencent QQ
 - QQ Wallet
 - WeChat
 - Alibaba products, including but not limited to:
 - AliPay
 - Kaspersky Lab

- 3) DOA-DET will, as soon as practicable, establish guidance, as well as utilize existing policies, standards, procedures, and processes, including the evaluation of necessary exceptions, related to applications or vendors, and will also provide updates related to the implementation of these directives, through the normal channels, including but not limited to DOA-DET's websites and updates to agency IT professionals.

- 4) DOA-DET, at the direction of the State CIO and State CISO, and in collaboration with the Governor, the Office of the Governor, and state, federal, and industry-led intelligence, will continually monitor and update the directives prescribed in this Order.
- 5) DOA-DET shall monitor adherence to issued guidance, policies, standards, procedures, and processes, where statutorily authorized, and shall assist impacted executive branch agencies to ensure they are able to abide by all technical standards and directives of DOA-DET and the State CIO and State CISO including but not limited to support with the following:
 - a. Developing and implementing a plan to remove any prohibited hardware products from State networks;
 - b. Removing any prohibited software products from State networks;
 - c. Implementing measures to prevent the installation of prohibited hardware and software products on State-owned, State-leased, or State-managed technology assets;
 - d. Implementing network-based restrictions to prevent the use of, or access to, prohibited services; and
 - e. Incorporating the risks associated with these technologies into statewide cybersecurity and awareness training programs.
- 6) In addition to the above provisions related to DOA-DET, executive branch agencies headed by individuals appointed by the Governor shall interpret any DOA-DET issued policy, procedure, or process prohibiting use of an application or vendor to extend to use of that application or vendor for marketing or advertising strategies, including those implemented by a third party.



IN TESTIMONY WHEREOF, I have hereunto set my hand and caused the Great seal of the State of Wisconsin to be affixed. Done at the Capitol in the City of Madison this eleventh day of January in the year of two thousand twenty-three.

TONY EVERS
Governor

By the Governor:

DOUGLAS LA FOLLETTE

Secretary of State