House Health and Government Operations Committee
House Bill 617
State Information Technology - Prohibited Applications and Websites
February 13, 2024

Chair Pena-Melnyk, Vice Chair Cullison and committee members, thank you for the opportunity to share our position on House Bill 617. The bill bans the downloading and use of all products by ByteDance Ltd. and TenCent Holdings Ltd. from all state-owned information technology, including all devices and networks.

The University System of Maryland (USM) comprises 12 distinguished universities and three regional centers with distinct and unique approaches to the mission of educating students and promoting the economic, intellectual, and cultural growth of its surrounding community. These institutions are located throughout the state, from Western Maryland to the Eastern Shore. A range of institutional types complement this geographic diversity. The USM includes land-grant universities, regional universities, and HBCUs, together with universities whose missions focus on online education, professional and graduate education, and environmental education.

The Chancellor, USM Presidents, and the Board of Regents all understand the importance of protecting information and technological systems from foreign government hacking and monitoring and have found it's best to take a risk-based approach in the USM. The ability to tailor our environment to support the use of technology and information in low-risk situations while restricting and protecting our technology and information in high-risk situations is crucial. The USM believes strongly that it is best to pursue a more flexible approach than House Bill 617, as written, allows.

The global cybersecurity threat landscape is constantly evolving, and it is well known that, in addition to ByteDance Ltd. and TenCent Holdings Ltd., many other companies and applications are owned and influenced by foreign adversaries. For example, Telegram Messenger and Kaspersky Labs have known ties to the Russian government; and Pinduoduo, Alibaba, Huawei, and ZTE also have ties to the Chinese government.

Given how quickly new technologies are developed and existing technologies evolve and change names; it may make more sense for the state to establish and maintain a list of companies, applications, and hardware solutions that pose a threat to Maryland. This list

could operate similarly to the way the US Department of State monitors global threats and maintains their Travel Advisories list. The Maryland Code could be used to establish and allocate resources to maintain a global technology advisory list, while the list itself is kept outside of the Maryland Code. The Maryland Department of Information Technology already operates the Office of Security Management (OSM) and the Maryland Information Sharing and Analysis Center (MD-ISAC). The OSM and the MD-ISAC could be logical groups to establish and maintain a global technology advisory list on behalf of all state units.

The solution we are suggesting is in line with the direction that the federal government began discussing last spring. On March 7, 2023, Congress introduced the RESTRICT Act. The bill requires federal actions to identify and mitigate foreign threats to information and communications technology (ICT) products and services (e.g., social media applications). Specifically, the US Department of Commerce must identify, deter, disrupt, prevent, prohibit, investigate, and mitigate transactions involving ICT products and services (1) in which any foreign adversary (such as China) has any interest, and (2) that pose an undue or unacceptable risk to U.S. national security or the safety of U.S. persons. The RESTRICT Act moves away from naming specific companies and products in statute or regulation and creates a structure to monitor and take appropriate steps to address the influence of foreign adversaries on our technology. We are suggesting that House Bill 617 be amended to operate similarly.

Lastly, instead of banning the use of particular technologies by state units, we recommend that House Bill 617 require all state units or entities contracting with a state unit perform an analysis of the risks and benefits posed by high-risk technologies on the state's technology advisory list, and as necessary put in place appropriate controls to address each risk. The controls a unit decides are best to address a risk can include banning the technology; but if necessary, it could also include more nuanced controls. Compliance with this provision could be included in IT audits performed by the Maryland Office of Legislative Audits.

In the end, we all agree that we need to protect the state from the risks posed by foreign adversaries and malicious actors in general. The structure we have outlined above is forward looking and creates a solution that can evolve over time, provides the flexibility to keep up with the fast pace of the cybersecurity threat landscape, allows units to implement appropriate controls while still serving their communities, and includes checks and balances to hold state units accountable.

USM Office of Government Relations – Susan Lawrence: slawrence@usmd.edu