WEST VIRGINIA LEGISLATURE

2023 REGULAR SESSION

ENGROSSED

Committee Substitute

for

Senate Bill 426

BY SENATORS BLAIR (MR. PRESIDENT) AND WOELFEL

[Originating in the Committee on the Judiciary;

reported on January 25, 2023]

A BILL to amend the Code of West Virginia, 1931, as amended, by adding thereto a new section, designated §5A-6B-4a, relating to regulating, restricting, or banning high-risk technology platforms, services, applications, programs, or products on government networks, devices, and systems; adding legislative findings related to national security threats and threats to critical state government networks and infrastructure posed by untrustworthy and high-risk platforms, services, applications, programs, or products; authorizing the Chief Information Security Officer to identify high-risk platforms, services, applications, programs, and products and to develop statewide standards regulating their use on government networks, devices, and systems; requiring certain government entities to adopt and enforce those standards; and authorizing the promulgation of legislative and emergency rules to facilitate the purpose of this section.

Be it enacted by the Legislature of West Virginia:

ARTICLE 6B. CYBER SECURITY PROGRAM.

§5A-6B-4a. High-risk platforms, services, applications, programs, and products.

(a) The Legislature hereby finds and declares that it is in the best interest of the citizens of West Virginia and to national security to enact measures designed to safeguard against untrustworthy and high-risk technology and to block such technology from interfering with or damaging critical state networks and infrastructure. The use of certain information and communication technologies and services can create opportunities for foreign adversaries to exploit vulnerabilities and take adverse action against the United States or allies, which could directly or indirectly affect the safety and security of West Virginia citizens, and such use also create opportunities for adversaries to exploit vulnerabilities and take adverse action against state or local government networks and infrastructure within or connected to West Virginia. As the threat landscape evolves, West Virginia shall work in cooperation with the federal government to implement appropriate safeguards to defend government networks in West Virginia and in the United States from foreign technology threats.

(b) Notwithstanding the provision of §5A-6B-1(b) of this code, all state agencies, including without limitation agencies within the executive, legislative, and judicial branches, all constitutional officers, local government entities as defined by §7-1-1 *et seq.* or §8-1-2 of this code, county boards of education as defined by §18-1-1 *et seq.* of this code, and all state institutions of higher education as defined by §18B-1-2 of this code, shall enforce statewide standards developed by the Chief Information Security Officer regarding high-risk technology platforms, services, applications, programs, or products. Additionally, all government entities subject to this subsection must, consistent with those standards and any other applicable state or federal law, restrict, remove, ban or otherwise block access to high-risk technology platforms, services, applications, programs, or products on all government systems, services, networks, devices, or locations. For purposes of this subsection, high-risk technology platforms, services, applications, programs, or products are those designated as such in the Statewide Cybersecurity Standard published and maintained by the Chief Information Security Officer, and shall include TikTok. Provided, any standards developed by the Chief Information Security Officer regarding high-risk technology platforms, services, applications, programs, or products shall contain exceptions permitting, in appropriate circumstances, the use of those platforms, services, applications, programs, or products for law enforcement activities, national security interests and activities, security research, investigative efforts authorized by this code, and for other purposes related to actual or potential litigation involving the state or one of its agencies or officers; and provided further, that the Chief Information Security Officer shall develop standards and requirements designed to mitigate the risk of any such authorized use of a high-risk platform, service, application, program, or product pursuant to the exceptions set forth in this section.

(c) The Secretary of the Department of Administration may propose rules for legislative approval in accordance with the provisions of §29A-3-1 *et seq*. of this code and may also promulgate emergency rules pursuant to the provisions of §29A-3-15 of this code when necessary to facilitate completion of the duties imposed on the Chief Information Security Officer by and enforcement of the standards referenced in this section.