WEST VIRGINIA LEGISLATURE

2023 REGULAR SESSION

Introduced

House Bill 2898

By Delegates Hanshaw (Mr. Speaker), Skaff and

Coop-Gonzalez

[By Request Of The Executive]

[Introduced January 23, 2023; Referred to the

Committee on Technology and Infrastructure then the

Judiciary]

A BILL to amend the Code of West Virginia, 1931, as amended, by adding thereto a new section, designated §5A-6B-4a, relating to banning high-risk technologies on government systems; adding legislative findings related to national security threats posed by untrustworthy or high-risk platforms and programs; and requiring certain government entities to adopt statewide standards that ban the use of high-risk platforms and products on government systems.

Be it enacted by the Legislature of West Virginia:

ARTICLE 6B. CYBER SECURITY PROGRAM.

§5A-6B-4a. High-risk technology ban.

(a) The Legislature hereby finds and declares that it is in the best interest of the citizens of West Virginia and to the national security to enact measures designed to purge and prevent untrustworthy and high-risk 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. 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 or §8-1-2 of this code, county boards of education as defined by §18-1-1 of this code, and higher education institutions, shall enforce statewide standards developed by the Chief Information Security Officer regarding banned high-risk technology platforms or products. Additionally, all government entities subject to this subsection must remove, restrict, and ban those high-risk technology platforms or products that pose a cybersecurity threat from all government systems, services, networks, devices, or

locations. For purposes of this subsection, high-risk technology platforms or products are those designated as such in the Statewide Cybersecurity Standard published and maintained by the Chief Information Security Officer.

NOTE: The purpose of this bill is to prevent cybersecurity threats to critical government networks and infrastructure by banning the use of certain products and platforms that have been deemed unsafe or high-risk. This bill requires West Virginia government entities to adopt and abide by the standards set forth by the Chief Information Security Officer and stay up to date with federal law and regulations pertaining to cybersecurity threats.

Strike-throughs indicate language that would be stricken from a heading or the present law and underscoring indicates new language that would be added.