24106781D

SENATE BILL NO. 222

AMENDMENT IN THE NATURE OF A SUBSTITUTE

(Proposed by the Senate Committee on General Laws and Technology on February 7, 2024)

(Patron Prior to Substitute—Senator McGuire)

A BILL to amend and reenact § 2.2-5514 of the Code of Virginia, relating to Commonwealth information security requirements.

Be it enacted by the General Assembly of Virginia:

1. That § 2.2-5514 of the Code of Virginia is amended and reenacted as follows:

§ 2.2-5514. Prohibited products and services and required incident reporting.

A. ~~For the purposes of this section, "public~~ *As used in this chapter, unless the context requires a different meaning:*

"Cybersecurity information" means information describing or relating to any security system or measure, whether manual or automated, that is used to control access to or use of information technology; security risks, threats, or vulnerabilities involving information technology; or security preparedness, response, or recovery related to information technology. "Cybersecurity information" includes critical infrastructure information and information regarding cybersecurity risks, cybersecurity threats, and incidents, as those terms are defined in 6 U.S.C. § 650.

"Public body" means any legislative body; any court of the Commonwealth; any authority, board, bureau, commission, district, or agency of the Commonwealth; any political subdivision of the Commonwealth, including counties, cities, and towns, city councils, boards of supervisors, school boards, planning commissions, and governing boards of institutions of higher education; and other organizations, corporations, or agencies in the Commonwealth supported wholly or principally by public funds. "Public body" includes any committee, subcommittee, or other entity however designated of the public body or formed to advise the public body, including those with private sector or citizen members and corporations organized by the Virginia Retirement System.

B. No public body may use, whether directly or through work with or on behalf of another public body, any hardware, software, or services that have been prohibited by the U.S. Department of Homeland Security for use on federal systems.

C. Every public body shall report all (i) known incidents that threaten the security of the Commonwealth's data or communications or result in exposure of data protected by federal or state laws and (ii) other incidents compromising the security of the public body's information technology systems with the potential to cause major disruption to normal activities of the public body or other public bodies. Such reports shall be made to the Virginia Fusion Intelligence Center within 24 hours from when the incident was discovered. The Virginia Fusion Intelligence Center shall share such reports with the Chief Information Officer, as described in § 2.2-2005, or his designee at the Virginia Information Technologies Agency, promptly upon receipt.

D. No cybersecurity information received by the Virginia Information Technologies Agency (VITA) shall be subject to the Virginia Freedom of Information Act (§ 2.2-3700 et seq.) or the Government Data Collection and Dissemination Practices Act (§ 2.2-3800 et seq.) while in the possession of VITA, neither transferring cybersecurity information to nor sharing cybersecurity information with VITA shall make VITA the custodian of such information for public records purposes. No provision of cybersecurity information to state agencies shall constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection. Persons having access to cybersecurity information maintained by VITA shall keep such information confidential, and no person or agency receiving cybersecurity information from VITA shall release or disseminate such information without prior authorization. The Chief Information Officer, as pursuant to § 2.2-2005, or his designee may authorize publication or disclosure of reports or aggregate cybersecurity information as appropriate.