23102473D

HOUSE BILL NO. 2385

Offered January 16, 2023

A BILL to amend and reenact §§ 2.2-2009 and 23.1-1017 of the Code of Virginia and to amend the Code of Virginia by adding a section numbered 2.2-4321.4 and by adding in Chapter 55.3 of Title 2.2 a section numbered 2.2-5514.1, relating to administration of state government; prohibited actions; civil penalty.

Patron—Brewer

Referred to Committee on Communications, Technology and Innovation

Be it enacted by the General Assembly of Virginia:

1. That §§ 2.2-2009 and 23.1-1017 of the Code of Virginia are amended and reenacted and that the Code of Virginia is amended by adding a section numbered 2.2-4321.4 and by adding in Chapter 55.3 of Title 2.2 a section numbered 2.2-5514.1 as follows:

§ 2.2-2009. Additional duties of the CIO relating to security of government information.

A. To provide for the security of state government electronic information from unauthorized uses, intrusions or other security threats, the CIO shall direct the development of policies, standards, and guidelines for assessing security risks, determining the appropriate security measures and performing security audits of government electronic information. Such policies, standards, and guidelines shall apply to the Commonwealth's executive, legislative, and judicial branches and independent agencies. The CIO shall work with representatives of the Chief Justice of the Supreme Court and Joint Rules Committee of the General Assembly to identify their needs. Such policies, standards, and guidelines shall, at a minimum:

1. Address the scope and frequency of security audits. In developing and updating such policies, standards, and guidelines, the CIO shall designate a government entity to oversee, plan, and coordinate the conduct of periodic security audits of all executive branch agencies and independent agencies. The CIO shall coordinate these audits with the Auditor of Public Accounts and the Joint Legislative Audit and Review Commission. The Chief Justice of the Supreme Court and the Joint Rules Committee of the General Assembly shall determine the most appropriate methods to review the protection of electronic information within their branches;

2. Control unauthorized uses, intrusions, or other security threats;

3. Provide for the protection of confidential data maintained by state agencies against unauthorized access and use in order to ensure the security and privacy of citizens of the Commonwealth in their interaction with state government. Such policies, standards, and guidelines shall include requirements that (i) any state employee or other authorized user of a state technology asset provide passwords or other means of authentication to use a technology asset and access a state-owned or state-operated computer network or database and (ii) a digital rights management system or other means of authenticating and controlling an individual's ability to access electronic records be utilized to limit access to and use of electronic records that contain confidential information to authorized individuals;

4. Address the creation and operation of a risk management program designed to identify information technology security gaps and develop plans to mitigate the gaps. All agencies in the Commonwealth shall cooperate with the CIO, including (i) providing the CIO with information required to create and implement a Commonwealth risk management program, (ii) creating an agency risk management program, and (iii) complying with all other risk management activities; and

5. Require that any contract for information technology entered into by the Commonwealth's executive, legislative, and judicial branches and independent agencies require compliance with applicable federal laws and regulations pertaining to information security and privacy.

B. 1. The CIO shall annually report to the Governor, the Secretary, and General Assembly on the results of security audits, the extent to which security policy, standards, and guidelines have been adopted by executive branch and independent agencies, and a list of those executive branch agencies and independent agencies that have not implemented acceptable security and risk management regulations, policies, standards, and guidelines to control unauthorized uses, intrusions, or other security threats. For any executive branch agency or independent agency whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to (i) the Secretary, (ii) any other affected cabinet secretary, (iii) the Governor, and (iv) the Auditor of Public Accounts. Upon review of the security audit results in question, the CIO may take action to suspend the executive branch agency's or independent agency's information technology projects pursuant to subsection B of § 2.2-2016.1, limit additional information technology investments pending acceptable corrective actions, and recommend to

the Governor and Secretary any other appropriate actions.

2. Executive branch agencies and independent agencies subject to such audits as required by this section shall fully cooperate with the entity designated to perform such audits and bear any associated costs. Public bodies that are not required to but elect to use the entity designated to perform such audits shall also bear any associated costs.

C. In addition to coordinating security audits as provided in subdivision B 1, the CIO shall conduct an annual comprehensive review of cybersecurity policies of every executive branch agency, with a particular focus on any breaches in information technology that occurred in the reviewable year and any steps taken by agencies to strengthen cybersecurity measures. Upon completion of the annual review, the CIO shall issue a report of his findings to the Chairmen of the House Committee on Appropriations and the Senate Committee on Finance and Appropriations. Such report shall not contain technical information deemed by the CIO to be security sensitive or information that would expose security vulnerabilities.

D. The provisions of this section shall not infringe upon responsibilities assigned to the Comptroller, the Auditor of Public Accounts, or the Joint Legislative Audit and Review Commission by other provisions of the Code of Virginia.

E. The CIO shall promptly receive reports from public bodies in the Commonwealth made in accordance with § 2.2-5514 and shall take such actions as are necessary, convenient, or desirable to ensure the security of the Commonwealth's electronic information and confidential data.

F. The CIO shall provide technical guidance to the Department of General Services in the development of policies, standards, and guidelines for the recycling and disposal of computers and other technology assets. Such policies, standards, and guidelines shall include the expunging, in a manner as determined by the CIO, of all confidential data and personal identifying information of citizens of the Commonwealth prior to such sale, disposal, or other transfer of computers or other technology assets.

G. The CIO shall provide all directors of agencies and departments with all such information, guidance, and assistance required to ensure that agencies and departments understand and adhere to the policies, standards, and guidelines developed pursuant to this section.

H. The CIO shall promptly notify all public bodies as defined in § 2.2-5514 of hardware, software, or services that have been prohibited pursuant to Chapter 55.3 (§ 2.2-5514 *et seq.*). *The CIO shall restrict access to prohibited applications and websites in accordance with the provisions of § 2.2-5514.1.*

I. 1. This subsection applies to the Commonwealth's executive, legislative, and judicial branches and independent agencies.

2. In collaboration with the heads of executive branch and independent agencies and representatives of the Chief Justice of the Supreme Court and the Joint Rules Committee of the General Assembly, the CIO shall develop and annually update a curriculum and materials for training all state employees in information security awareness and in proper procedures for detecting, assessing, reporting, and addressing information security threats. The curriculum shall include activities, case studies, hypothetical situations, and other methods of instruction (i) that focus on forming good information security habits and procedures among state employees and (ii) that teach best practices for detecting, assessing, reporting, and addressing information security threats.

3. Every state agency shall provide annual information security training for each of its employees using the curriculum and materials developed by the CIO pursuant to subdivision 2. Employees shall complete such training within 30 days of initial employment and by January 31 each year thereafter.

State agencies may develop additional training materials that address specific needs of such agency, provided that such materials do not contradict the training curriculum and materials developed by the CIO.

The CIO shall coordinate with and assist state agencies in implementing the annual information security training requirement.

4. Each state agency shall (i) monitor and certify the training activity of its employees to ensure compliance with the annual information security training requirement, (ii) evaluate the efficacy of the information security training program, and (iii) forward to the CIO such certification and evaluation, together with any suggestions for improving the curriculum and materials, or any other aspects of the training program. The CIO shall consider such evaluations when it annually updates its curriculum and materials.

§ 2.2-4321.4. Prohibited contracts; Government of China; civil penalty.

A. As used in this section, unless the context requires a different meaning:

"Committee on Foreign Investment in the United States" means an interagency committee (i) operated pursuant to § 721 of the Defense Production Act of 1950 (50 U.S.C. § 4501 et seq.), as amended, and as implemented by Executive Order 11858, as amended, and the regulations set forth in 31 C.F.R. § 800 and (ii) authorized to (a) review certain real estate transactions by foreign persons in order to determine the effect of such transactions on the national security of the United States and (b)

respond to new and emerging threats and vulnerabilities in the context of foreign investments.

"Company" means any sole proprietorship, organization, association, corporation, partnership, joint venture, limited partnership, limited liability partnership, limited liability company, or other entity or business association, including all wholly owned subsidiaries, majority owned subsidiaries, parent companies, or affiliates of such entities or business associations, that exists for the purpose of making a profit.

"Government of China" means the government of the People's Republic of China led by the Chinese Communist Party.

"Scrutinized company" means any company owned or operated by the Government of China, other than a company for which the Committee on Foreign Investment in the United States has determined that there are no unresolved national security concerns regarding the transaction that created such ownership or permitted such operation.

"State agency" means any authority, board, department, instrumentality, institution, agency, or other unit of state government. "State agency" does not include any locality or local or regional governmental authority.

B. No state agency shall contract for goods or services with a scrutinized company or any affiliate of a scrutinized company. A scrutinized company shall be prohibited from bidding on or submitting a proposal, directly or indirectly through a third party, for a contract with any state agency.

C. A state agency shall require any company that submits a bid or proposal with respect to a contract for goods or services to certify in writing that the company is not a scrutinized company. If the state agency determines that the company has falsified information in submitting such certification, (i) the state agency shall terminate the contract with the company, (ii) the company shall be prohibited from bidding on any future state contracts, and (iii) the company shall be liable for a civil penalty in an amount equal to the greater of $250,000 or twice the amount of the contract for which the bid or proposal was submitted.

§ 2.2-5514.1. Prohibited applications and websites.

A. For the purposes of this section, unless the context requires a different meaning:

"ByteDance Ltd." means the Chinese internet technology company founded by Zhang Yiming and Liang Rubo in 2012, and any successor company or entity owned by such company.

"Executive branch agency" or "agency" means the same as that term is defined in § 2.2-2006.

"Tencent Holdings Ltd." means the Chinese multinational technology and entertainment conglomerate and holding company headquartered in Shenzhen, China, and any successor company or entity owned by such company.

"TikTok" means the video-sharing application developed by ByteDance Ltd. that hosts user-submitted videos.

"WeChat" means the multi-purpose social media, messaging, and payment application developed by Tencent Holdings Ltd.

B. Except as provided in subsection C, no employee or agent of any executive branch agency or person or entity contracting with any such agency shall download or use any application, including TikTok or WeChat, or access any website developed by ByteDance Ltd. or Tencent Holdings Ltd. (i) on any state-issued device or state-owned or state-leased equipment, including mobile phones, desktop computers, laptop computers, tablets, or other devices capable of connecting to the Internet, or (ii) while connected to any wired or wireless Internet network owned, operated, or maintained by the Commonwealth.

C. The Superintendent of State Police or the chief law-enforcement officer of the appropriate county or city may grant an exception to the provisions of subsection B for the purpose of allowing any employee, agent, person, or entity to participate in any law-enforcement-related matters.

§ 23.1-1017. Covered institutions; operational authority; procurement.

A. Subject to the express provisions of the management agreement, each covered institution may be exempt from the provisions of the Virginia Public Procurement Act (§ 2.2-4300 et seq.), except for §§ *2.2-4321.4*, 2.2-4340, 2.2-4340.1, 2.2-4340.2, 2.2-4342, and 2.2-4376.2, which shall not be construed to require compliance with the prequalification application procedures of subsection B of § 2.2-4317, provided, however, that (i) any deviations from the Virginia Public Procurement Act in the management agreement shall be uniform across all covered institutions and (ii) the governing board of the covered institution shall adopt, and the covered institution shall comply with, policies for the procurement of goods and services, including professional services, that shall (a) be based upon competitive principles; (b) in each instance seek competition to the maximum practical degree; (c) implement a system of competitive negotiation for professional services pursuant to §§ 2.2-4303.1 and 2.2-4302.2; (d) prohibit discrimination in the solicitation and award of contracts on the basis of the bidder's or offeror's race, religion, color, sex, sexual orientation, gender identity, national origin, age, or disability or on any other basis prohibited by state or federal law; (e) incorporate the prompt payment principles of §§ 2.2-4350

and 2.2-4354; (f) consider the impact on correctional enterprises under § 53.1-47; and (g) provide that whenever solicitations are made seeking competitive procurement of goods or services, it shall be a priority of the institution to provide for fair and reasonable consideration of small, women-owned, and minority-owned businesses and to promote and encourage a diversity of suppliers.

B. Such policies may (i) provide for consideration of the dollar amount of the intended procurement, the term of the anticipated contract, and the likely extent of competition; (ii) implement a prequalification procedure for contractors or products; and (iii) include provisions for cooperative arrangements with other covered institutions, other public or private educational institutions, or other public or private organizations or entities, including public-private partnerships, public bodies, charitable organizations, health care provider alliances or purchasing organizations or entities, state agencies or institutions of the Commonwealth or the other states, the District of Columbia, the territories, or the United States, and any combination of such organizations and entities.

C. Nothing in this section shall preclude a covered institution from requesting and utilizing the assistance of the Virginia Information Technologies Agency for information technology procurements and covered institutions are encouraged to utilize such assistance.

D. Each covered institution shall post on the Department of General Services' central electronic procurement website all Invitations to Bid, Requests for Proposal, sole source award notices, and emergency award notices to ensure visibility and access to the Commonwealth's procurement opportunities on one website.

E. As part of any procurement provisions of the management agreement, the governing board of a covered institution shall identify the public, educational, and operational interests served by any procurement rule that deviates from procurement rules in the Virginia Public Procurement Act (§ 2.2-4300 et seq.).