

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.

Patrons—Brewer, Austin, Avoli, Ballard, Bloxom, Byron, Campbell, E.H., Campbell, J.L., Cherry, Cordoza, Durant, Fowler, Greenhalgh, Head, Hodges, Kilgore, LaRock, Leftwich, McGuire, McNamara, O'Quinn, Orrock, Robinson, Runion, Tata, Taylor, Walker, Wampler, Ware, Wiley, Williams, Wright and Wyatt

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

INTRODUCED

HB2385

56 security audit results in question, the CIO may take action to suspend the executive branch agency's or  
57 independent agency's information technology projects pursuant to subsection B of § 2.2-2016.1, limit  
58 additional information technology investments pending acceptable corrective actions, and recommend to  
59 the Governor and Secretary any other appropriate actions.

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

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

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

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

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

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

86 H. The CIO shall promptly notify all public bodies as defined in § 2.2-5514 of hardware, software,  
87 or services that have been prohibited pursuant to Chapter 55.3 (§ 2.2-5514 *et seq.*). *The CIO shall*  
88 *restrict access to prohibited applications and websites in accordance with the provisions of §*  
89 *2.2-5514.1.*

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

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

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

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

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

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

114 **§ 2.2-4321.4. Prohibited contracts; Government of China; civil penalty.**

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

116 "Committee on Foreign Investment in the United States" means an interagency committee (i)  
117 operated pursuant to § 721 of the Defense Production Act of 1950 (50 U.S.C. § 4501 *et seq.*), as

118 amended, and as implemented by Executive Order 11858, as amended, and the regulations set forth in  
 119 31 C.F.R. § 800 and (ii) authorized to (a) review certain real estate transactions by foreign persons in  
 120 order to determine the effect of such transactions on the national security of the United States and (b)  
 121 respond to new and emerging threats and vulnerabilities in the context of foreign investments.

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

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

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

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

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

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

146 **§ 2.2-5514.1. Prohibited applications and websites.**

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

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

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

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

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

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

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

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

168 **§ 23.1-1017. Covered institutions; operational authority; procurement.**

169 A. Subject to the express provisions of the management agreement, each covered institution may be  
 170 exempt from the provisions of the Virginia Public Procurement Act (§ 2.2-4300 et seq.), except for §§  
 171 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  
 172 require compliance with the prequalification application procedures of subsection B of § 2.2-4317,  
 173 provided, however, that (i) any deviations from the Virginia Public Procurement Act in the management  
 174 agreement shall be uniform across all covered institutions and (ii) the governing board of the covered  
 175 institution shall adopt, and the covered institution shall comply with, policies for the procurement of  
 176 goods and services, including professional services, that shall (a) be based upon competitive principles;  
 177 (b) in each instance seek competition to the maximum practical degree; (c) implement a system of  
 178 competitive negotiation for professional services pursuant to §§ 2.2-4303.1 and 2.2-4302.2; (d) prohibit

179 discrimination in the solicitation and award of contracts on the basis of the bidder's or offeror's race,  
180 religion, color, sex, sexual orientation, gender identity, national origin, age, or disability or on any other  
181 basis prohibited by state or federal law; (e) incorporate the prompt payment principles of §§ 2.2-4350  
182 and 2.2-4354; (f) consider the impact on correctional enterprises under § 53.1-47; and (g) provide that  
183 whenever solicitations are made seeking competitive procurement of goods or services, it shall be a  
184 priority of the institution to provide for fair and reasonable consideration of small, women-owned, and  
185 minority-owned businesses and to promote and encourage a diversity of suppliers.

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

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

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

201 E. As part of any procurement provisions of the management agreement, the governing board of a  
202 covered institution shall identify the public, educational, and operational interests served by any  
203 procurement rule that deviates from procurement rules in the Virginia Public Procurement Act (§  
204 2.2-4300 et seq.).