

23103506D

SENATE BILL NO. 1459

Senate Amendments in [] - February 6, 2023

A *BILL to amend and reenact § 2.2-2009 of the Code of Virginia and to amend the Code of Virginia by adding in Chapter 55.3 of Title 2.2 a section numbered 2.2-5514.1, relating to administration of state government; prohibited applications and websites.*

Patrons Prior to Engrossment—Senators McDougle, Cosgrove, DeSteph, Dunnavant, Hackworth, Hanger, Newman, Norment, Obenshain, Peake, Pillion, Reeves, Ruff, Stanley, Stuart and Vogel

Referred to Committee on General Laws and Technology

Be it enacted by the General Assembly of Virginia:

1. That § 2.2-2009 of the Code of Virginia is amended and reenacted and that the Code of Virginia is amended 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.

ENGROSSED

SBI459E

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

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

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

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

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

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

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

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

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

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

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

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

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

111 **§ 2.2-5514.1. Prohibited applications and websites.**

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

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

115 ["~~Executive branch agency~~" or "~~agency~~" "~~Public body~~"] means the same as that term is defined in
116 § [2.2-2006 2.2-5514].

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

120 "TikTok" means the video-sharing application developed [~~and owned~~] by ByteDance Ltd. that hosts
121 user-submitted videos.

122 "WeChat" means the multi-purpose social media, messaging, and payment application developed [
123 ~~and owned~~] by Tencent Holdings Ltd.

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

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

ENGROSSED

SB1459E