VIRGINIA ACTS OF ASSEMBLY — CHAPTER

An Act 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.

[S 1459]

Approved

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.

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

57 costs. Public bodies that are not required to but elect to use the entity designated to perform such audits
58 shall also bear any associated costs.
59   C. In addition to coordinating security audits as provided in subdivision B 1, the CIO shall conduct
60 an annual comprehensive review of cybersecurity policies of every executive branch agency, with a
61 particular focus on any breaches in information technology that occurred in the reviewable year and any
62 steps taken by agencies to strengthen cybersecurity measures. Upon completion of the annual review, the
63 CIO shall issue a report of his findings to the Chairmen of the House Committee on Appropriations and
64 the Senate Committee on Finance and Appropriations. Such report shall not contain technical
65 information deemed by the CIO to be security sensitive or information that would expose security
66 vulnerabilities.
67   D. The provisions of this section shall not infringe upon responsibilities assigned to the Comptroller,
68 the Auditor of Public Accounts, or the Joint Legislative Audit and Review Commission by other
69 provisions of the Code of Virginia.
70   E. The CIO shall promptly receive reports from public bodies in the Commonwealth made in
71 accordance with § 2.2-5514 and shall take such actions as are necessary, convenient, or desirable to
72 ensure the security of the Commonwealth's electronic information and confidential data.
73   F. The CIO shall provide technical guidance to the Department of General Services in the
74 development of policies, standards, and guidelines for the recycling and disposal of computers and other
75 technology assets. Such policies, standards, and guidelines shall include the expunging, in a manner as
76 determined by the CIO, of all confidential data and personal identifying information of citizens of the
77 Commonwealth prior to such sale, disposal, or other transfer of computers or other technology assets.
78   G. The CIO shall provide all directors of agencies and departments with all such information,
79 guidance, and assistance required to ensure that agencies and departments understand and adhere to the
80 policies, standards, and guidelines developed pursuant to this section.
81   H. The CIO shall promptly notify all public bodies as defined in § 2.2-5514 of hardware, software,
82 or services that have been prohibited pursuant to Chapter 55.3 (§ 2.2-5514 *et seq.*). *The CIO shall*
83 *restrict access to prohibited applications and websites in accordance with the provisions of § 2.2-5514.1.*
84   I. 1. This subsection applies to the Commonwealth's executive, legislative, and judicial branches and
85 independent agencies.
86   2. In collaboration with the heads of executive branch and independent agencies and representatives
87 of the Chief Justice of the Supreme Court and the Joint Rules Committee of the General Assembly, the
88 CIO shall develop and annually update a curriculum and materials for training all state employees in
89 information security awareness and in proper procedures for detecting, assessing, reporting, and
90 addressing information security threats. The curriculum shall include activities, case studies, hypothetical
91 situations, and other methods of instruction (i) that focus on forming good information security habits
92 and procedures among state employees and (ii) that teach best practices for detecting, assessing,
93 reporting, and addressing information security threats.
94   3. Every state agency shall provide annual information security training for each of its employees
95 using the curriculum and materials developed by the CIO pursuant to subdivision 2. Employees shall
96 complete such training within 30 days of initial employment and by January 31 each year thereafter.
97   State agencies may develop additional training materials that address specific needs of such agency,
98 provided that such materials do not contradict the training curriculum and materials developed by the
99 CIO.
100   The CIO shall coordinate with and assist state agencies in implementing the annual information
101 security training requirement.
102   4. Each state agency shall (i) monitor and certify the training activity of its employees to ensure
103 compliance with the annual information security training requirement, (ii) evaluate the efficacy of the
104 information security training program, and (iii) forward to the CIO such certification and evaluation,
105 together with any suggestions for improving the curriculum and materials, or any other aspects of the
106 training program. The CIO shall consider such evaluations when it annually updates its curriculum and
107 materials.
108   *§ 2.2-5514.1. Prohibited applications and websites.*
109   *A. For the purposes of this section, unless the context requires a different meaning:*
110   *"ByteDance Ltd." means the Chinese internet technology company founded by Zhang Yiming and*
111 *Liang Rubo in 2012, and any successor company or entity owned by such company.*
112   *"Public body" means the same as that term is defined in § 2.2-5514.*
113   *"Tencent Holdings Ltd." means the Chinese multinational technology and entertainment conglomerate*
114 *and holding company headquartered in Shenzhen, China, and any successor company or entity owned*
115 *by such company.*
116   *"TikTok" means the video-sharing application developed by ByteDance Ltd. that hosts user-submitted*
117 *videos.*

118   *"WeChat" means the multipurpose social media, messaging, and payment application developed by*
119 *Tencent Holdings Ltd.*
120   *B. Except as provided in subsection C, no employee or agent of any public body or person or entity*
121 *contracting with any such public body shall download or use any application, including TikTok or*
122 *WeChat, or access any website developed by ByteDance Ltd. or Tencent Holdings Ltd. (i) on any*
123 *government-issued device or government-owned or government-leased equipment, including mobile*
124 *phones, desktop computers, laptop computers, tablets, or other devices capable of connecting to the*
125 *Internet, or (ii) while connected to any wired or wireless Internet network owned, operated, or*
126 *maintained by the Commonwealth.*
127   *C. The Superintendent of State Police or the chief law-enforcement officer of the appropriate locality*
128 *or institution of higher education may grant an exception to the provisions of subsection B for the*
129 *purpose of allowing any employee, agent, person, or entity to participate in any law-enforcement-related*
130 *matters.*

REENROLLED

SB1459ER2