24103126D

SENATE BILL NO. 222

Offered January 10, 2024

Prefiled January 8, 2024

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 2.2-5514.2, relating to Commonwealth information security requirements.

Patron—McGuire

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 2.2-5514.2 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 *and shall publish and maintain a list of such security policies and standards with which compliance is required for state public bodies pursuant to § 2.2-5514.2*. 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.

§ 2.2-5514.2. Commonwealth information security requirements.

A. For purposes of this section:

"CIO" means the same as that term is defined in § 2.2-2005.

"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 the same as that term is defined in § 2.2-5514.

"State public body" means any public body that is (i) listed in the appropriation act (ii) a public institution of higher education, as that term is defined in § 23.1-100, (iii) a political subdivision of the Commonwealth created in Chapter 22 (§ 2.2-2200 et seq.), (iv) the Virginia College Building Authority, (v) the Virginia Housing Development Authority, (vi) the Virginia Cannabis Control Authority, (vii) the Assistive Technology Loan Fund Authority, (viii) the Virginia Health Workforce Development Authority, (ix) the Online Virginia Network Authority, or (x) the Virginia Resources Authority.

B. Notwithstanding any exemption from Chapter 20.1 (§ 2.2-2005 et seq.), including an exemption pursuant to § 23.1-1018, all state public bodies shall comply with the requirements of this section.

1. Each state public body shall comply with the requirements of the Commonwealth's security policies and standards developed pursuant to subsection A of § 2.2-2009.

2. Each state public body shall ensure each of its employees completes information security training compliant with subsection I of § 2.2-2009.

3. Each state public body shall conduct regular security audits, the scope of which shall include the state public body's compliance with the Commonwealth's security policies and standards.

4. Legislative and judicial branch state public bodies shall annually report to the General Assembly on their security audit results; the extent to which Commonwealth security policies, standards, and guidelines have been adopted; and whether acceptable security and risk management regulations, policies, standards, and guidelines to control unauthorized uses, intrusions, or other security threats have been implemented. Any other state public body shall report such audit results to the CIO and cooperate with and be included in the CIO's reporting pursuant to subdivision B 1 of § 2.2-2009.

C. Cybersecurity information received by the Virginia Information Technologies Agency (VITA) shall not 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, and transferring cybersecurity information to or sharing cybersecurity information with VITA shall not make VITA the custodian of such information for public records purposes. The provision of cybersecurity information to state agencies, including under § 2.2-5514, shall not 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 CIO or his designee may authorize publication or disclosure of reports or cybersecurity information as appropriate.

2. That the Chief Information Officer of the Commonwealth shall (i) ensure that appropriate transition and implementation meetings with officials or personnel from a legislative or judicial branch state public body and any state public body previously exempt from the information security requirements occur, (ii) document any transition and implementation arrangements concerning requirements in the provisions of this act, and (iii) document any necessary or appropriate exemptions from the requirements of the provisions of this act.