20100246D

HOUSE BILL NO. 322

Offered January 8, 2020

Prefiled December 31, 2019

A BILL to amend and reenact §§ 2.2-2009 and 2.2-2101 of the Code of Virginia and to amend the Code of Virginia by adding a section numbered 2.2-2009.1, relating to the Virginia Information Technologies Agency; Cybersecurity Advisory Council created; report.

Patrons—Ayala, Carter, Davis, Samirah and Simonds

Referred to Committee on Communications, Technology and Innovation

Be it enacted by the General Assembly of Virginia:

1. That §§ 2.2-2009 and 2.2-2101 of the Code of Virginia are amended and reenacted and that the Code of Virginia is amended by adding a section numbered 2.2-2009.1 as follows:

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

A. To provide for the security of state government electronic information from unauthorized uses, intrusions, or other security threats, the CIO shall, *in consultation with the Cybersecurity Advisory Council established pursuant to § 2.2-2009.1,* 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 *the* General Assembly on *the work and recommendations of the Cybersecurity Advisory Council established pursuant to § 2.2-2009.1,* 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. 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 directors of departments in the executive branch of state government made in accordance with § 2.2-603 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).

§ 2.2-2009.1. Cybersecurity Advisory Council; purpose; membership; terms; compensation; report; staffing.

A. The Cybersecurity Advisory Council (the Advisory Council) is established as an advisory council in the executive branch of state government. The purpose of the Advisory Council is to (i) assist the CIO with the development of policies, standards, and guidelines for assessing security risks, determining appropriate security measures, and performing security audits of government electronic information; (ii) make recommendations to the CIO regarding strategies to strengthen the Commonwealth's cybersecurity; and (iii) analyze and investigate breaches of the information technology security of any independent agency or any agency or other entity within the executive, legislative, or judicial branch of state government.

B. The Advisory Council shall have a total membership of 13 members that shall consist of four legislative members, five nonlegislative citizen members, and four ex officio members. The Advisory Council's membership shall include three members of the House of Delegates, to be appointed by the Speaker of the House of Delegates in accordance with the principles of proportional representation contained in the Rules of the House of Delegates; one member of the Senate, to be appointed by the Senate Committee on Rules; and five nonlegislative citizen members to be appointed by the Governor, subject to confirmation by the General Assembly. The Director of the Division of Legislative Automated Systems, the Director of the Joint Legislative Audit and Review Commission, the Auditor of Public Accounts, and the Chief Justice of the Virginia Supreme Court, or their designees, shall serve ex officio with voting privileges. Nonlegislative citizen members of the Advisory Council shall be citizens of the Commonwealth.

Legislative members and ex officio members of the Advisory Council shall serve terms coincident with their terms of office. Appointments to fill vacancies, other than by expiration of a term, shall be for the unexpired terms. Vacancies shall be filled in the same manner as the original appointments.

After the initial staggering of terms, nonlegislative citizen members shall be appointed for a term of four years.

No House member shall serve more than four consecutive two-year terms, no Senate member shall serve more than two consecutive four-year terms, and no nonlegislative citizen member shall serve more than two consecutive four-year terms. The remainder of any term to which a member is appointed to fill a vacancy, or the expiration of a term of three years or less, shall not constitute a term in determining the member's eligibility for reappointment.

C. Legislative members of the Advisory Council shall receive such compensation as provided in § 30-19.12, and nonlegislative citizen members and ex officio members shall receive such compensation for the performance of their duties as provided in § 2.2-2813. All members shall be reimbursed for all reasonable and necessary expenses incurred in the performance of their duties as provided in §§ 2.2-2813 and 2.2-2825. Funding for the costs of compensation and expenses of the members shall be provided by VITA.

D. The Advisory Council shall elect a chairman and a vice-chairman from among its members. The Advisory Council meetings shall be held at least quarterly at the call of the chairman or whenever the majority of the members so request. A majority of the members shall constitute a quorum.

E. The Advisory Council shall submit to the Governor and the General Assembly no later than the first day of each regular session of the General Assembly an annual report on its activities for publication as a report document as provided in the procedures of the Division of Legislative Automated Systems for the processing of legislative documents and reports, which shall be posted on the General Assembly's website.

F. The Virginia Information Technologies Agency shall provide staff support to the Advisory Council. All agencies of the Commonwealth shall provide assistance to the Advisory Council, upon request.

§ 2.2-2101. Prohibition against service by legislators on boards, commissions, and councils within the executive branch; exceptions.

Members of the General Assembly shall be ineligible to serve on boards, commissions, and councils within the executive branch of state government who are responsible for administering programs established by the General Assembly. Such prohibition shall not extend to boards, commissions, and councils engaged solely in policy studies or commemorative activities. If any law directs the appointment of any member of the General Assembly to a board, commission, or council in the executive branch of state government that is responsible for administering programs established by the General Assembly, such portion of such law shall be void, and the Governor shall appoint another person from the Commonwealth at large to fill such a position.

The provisions of this section shall not apply to members of the Board for Branch Pilots, who shall be appointed as provided for in § 54.1-901; to members of the Board of Trustees of the Southwest Virginia Higher Education Center, who shall be appointed as provided for in § 23.1-3126; to members of the Board of Trustees of the Southern Virginia Higher Education Center, who shall be appointed as provided for in § 23.1-3121; to members of the Board of Directors of the New College Institute, who shall be appointed as provided for in § 23.1-3112; to members of the Advisory Board on Teacher Education and Licensure, who shall be appointed as provided for in § 22.1-305.2; to members of the Virginia Interagency Coordinating Council, who shall be appointed as provided for in § 2.2-5204; to members of the Board of Veterans Services, who shall be appointed as provided for in § 2.2-2452; to members appointed to the Board of Trustees of the Roanoke Higher Education Authority pursuant to § 23.1-3117; to members of the Board of Trustees of the Online Virginia Network Authority, who shall be appointed as provided in § 23.1-3136; to members of the Virginia Geographic Information Network Advisory Board, who shall be appointed as provided for in § 2.2-2423; to members of the Board of Visitors of the Virginia School for the Deaf and the Blind, who shall be appointed as provided for in § 22.1-346.2; to members of the Substance Abuse Services Council, who shall be appointed as provided for in § 2.2-2696; to members of the Criminal Justice Services Board, who shall be appointed as provided in § 9.1-108; to members of the State Executive Council for Children's Services, who shall be appointed as provided in § 2.2-2648; to members of the Virginia Board of Workforce Development, who shall be appointed as provided for in § 2.2-2471; to members of the Volunteer Firefighters' and Rescue Squad Workers' Service Award Fund Board, who shall be appointed as provided for in § 51.1-1201; to members of the Secure and Resilient Commonwealth Panel, who shall be appointed as provided for in § 2.2-222.3; to members of the Forensic Science Board, who shall be appointed as provided for in § 9.1-1109; to members of the Southwest Virginia Cultural Heritage Foundation, who shall be appointed as provided in § 2.2-2735; to members of the Virginia Growth and Opportunity Board, who shall be appointed as provided in § 2.2-2485; ~~or~~ to members of the Henrietta Lacks Commission, who shall be appointed as provided in § 2.2-2538*; or to members of the Cybersecurity Advisory Council, who shall be appointed as provided in § 2.2-2009.1*.

2. That the initial appointment by the Governor of nonlegislative citizen members of the Cybersecurity Advisory Council, as created by this act, shall be staggered as follows: one member for a term of one year, one member for a term of two years, one member for a term of three years, and two members for a term of four years.