19101788D

HOUSE BILL NO. 2519

Offered January 9, 2019

Prefiled January 9, 2019

A BILL to amend and reenact § 2.2-2009 of the Code of Virginia, relating to Virginia Information Technologies Agency; cybersecurity task force created.

Patrons—Ayala, Convirs-Fowler, Delaney, Hope, Kory, Lindsey, Lopez, Plum, Rasoul, Reid, Rodman and Simon

Referred to Committee on Science 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 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, *in consultation with the cybersecurity task force established pursuant to subsection B,* 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. *The CIO shall seek assistance in developing the policies, standards, and guidelines required pursuant to subsection A from a cybersecurity task force consisting of the following: representatives of the Chief Justice of the Supreme Court, representatives of the Joint Rules Committee of the General Assembly, the Director of the Division of Legislative Automated Systems or his designee, the Director of the Joint Legislative Audit and Review Commission or his designee, and the Auditor of Public Accounts or his designee. The CIO may request any other agency head to serve on or appoint a designee to serve on the task force. In addition to assisting the CIO in developing such policies, standards, and guidelines, the task force shall discuss and investigate any breaches in information technology security which have been experienced by any executive branch or independent agency, the legislative branch, or the judicial branch, and make recommendations for strengthening the Commonwealth's cybersecurity measures.*

The cybersecurity task force shall meet at least quarterly on such dates and times as the members determine. A majority of the task force shall constitute a quorum.

C. 1. The CIO shall annually report to the Governor, the Secretary, and General Assembly on *the work of the cybersecurity task force, including any recommendations made by the task force,* 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.~~ *D.* In addition to coordinating security audits as provided in subdivision ~~B~~ *C* 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.~~ *E.* 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.~~ *F.* 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.~~ *G.* 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.~~ *H.* 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.