16102176D

HOUSE BILL NO. 509

Offered January 13, 2016

Prefiled January 8, 2016

A BILL to amend and reenact §§ 2.2-603, 2.2-2006, 2.2-2007, and 2.2-2009 of the Code of Virginia, relating to security of government information; creation of the position of Chief Information Security Officer.

Patron—Boysko

Referred to Committee on Science and Technology

Be it enacted by the General Assembly of Virginia:

1. That §§ 2.2-603, 2.2-2006, 2.2-2007, and 2.2-2009 of the Code of Virginia are amended and reenacted as follows:

§ 2.2-603. Authority of agency directors.

A. Notwithstanding any provision of law to the contrary, the agency director of each agency in the executive branch of state government shall have the power and duty to (i) supervise and manage the department or agency and (ii) prepare, approve, and submit to the Governor all requests for appropriations and to be responsible for all expenditures pursuant to appropriations.

B. The director of each agency in the executive branch of state government, except those that by law are appointed by their respective boards, shall not proscribe any agency employee from discussing the functions and policies of the agency, without prior approval from his supervisor or superior, with any person unless the information to be discussed is protected from disclosure by the Virginia Freedom of Information Act (§ 2.2-3700 et seq.) or any other provision of state or federal law.

C. Subsection A shall not be construed to restrict any other specific or general powers and duties of executive branch boards granted by law.

D. This section shall not apply to those agency directors that are appointed by their respective boards or by the Board of Education. Directors appointed in this manner shall have the powers and duties assigned by law or by the board.

E. In addition to the requirements of subsection C of § 2.2-619, the director of each agency in any branch of state government shall, at the end of each fiscal year, report to (i) the Secretary of Finance and the Chairmen of the House Committee on Appropriations and the Senate Committee on Finance a listing and general description of any federal contract, grant, or money in excess of $1,000,000 for which the agency was eligible, whether or not the agency applied for, accepted, and received such contract, grant, or money, and, if not, the reasons therefore and the dollar amount and corresponding percentage of the agency's total annual budget that was supplied by funds from the federal government and (ii) the Chairmen of the House Committees on Appropriations and Finance, and the Senate Committee on Finance any amounts owed to the agency from any source that are more than six months delinquent, the length of such delinquencies, and the total of all such delinquent amounts in each six-month interval. Clause (i) shall not be required of public institutions of higher education.

F. Notwithstanding subsection D, the director of every agency and department in the executive branch of state government, including those appointed by their respective boards or the Board of Education, shall be responsible for securing the electronic data held by his agency or department and shall comply with the requirements of the Commonwealth's information technology security and risk-management program as set forth in § 2.2-2009.

G. The director of every department in the executive branch of state government shall report to the Chief Information *Security* Officer as ~~described~~ ~~in~~ ~~§ 2.2-2005,~~ *appointed pursuant to § 2.2-2009* all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal agency activities. Such reports shall be made to the Chief Information *Security* Officer within 24 hours from when the department discovered or should have discovered ~~their~~ occurrence *of any incident.*

§ 2.2-2006. Definitions.

As used in this chapter, unless the context requires a different meaning:

"CIO" means the Chief Information Officer of the Commonwealth.

"CISO" means the Chief Information Security Officer of the Commonwealth.

"Commonwealth information technology project" means any state agency information technology project that is under Commonwealth governance and oversight.

"Commonwealth Project Management Standard" means a document developed and adopted by the ~~Chief Information Officer (CIO)~~ *CIO* pursuant to § 2.2-2008 that describes the methodology for conducting information technology projects, and the governance and oversight used to ensure project success.

"Communications services" includes telecommunications services; automated data processing services; local, wide area, metropolitan, and all other data networks; and management information systems that serve the needs of state agencies and institutions.

"Confidential data" means information made confidential by federal or state law that is maintained by a state agency in an electronic format.

"Enterprise" means an organization with common or unifying business interests. An enterprise may be defined at the Commonwealth level or secretariat level for program and project integration within the Commonwealth, secretariats, or multiple agencies.

"Information technology" means telecommunications, automated data processing, applications, databases, the Internet, management information systems, and related information, equipment, goods, and services. The provisions of this chapter shall not be construed to hamper the pursuit of the missions of the institutions in instruction and research.

"ITAC" means the Information Technology Advisory Council created in § 2.2-2699.5.

"Major information technology project" means any Commonwealth information technology project that has a total estimated cost of more than $1 million or that has been designated a major information technology project by the CIO pursuant to the Commonwealth Project Management Standard developed under § 2.2-2008.

"Noncommercial telecommunications entity" means any public broadcasting station as defined in § 22.1-20.1.

"Public broadcasting services" means the acquisition, production, and distribution by public broadcasting stations of noncommercial educational, instructional, informational, or cultural television and radio programs and information that may be transmitted by means of electronic communications, and related materials and services provided by such stations.

"Public telecommunications entity" means any public broadcasting station as defined in § 22.1-20.1.

"Public telecommunications facilities" means all apparatus, equipment and material necessary for or associated in any way with public broadcasting stations as defined in § 22.1-20.1 or public broadcasting services, including the buildings and structures necessary to house such apparatus, equipment and material, and the necessary land for the purpose of providing public broadcasting services, but not telecommunications services.

"Public telecommunications services" means public broadcasting services.

"Secretary" means the Secretary of Technology.

"State agency" or "agency" means any agency, institution, board, bureau, commission, council, or instrumentality of state government in the executive branch listed in the appropriation act. However, the terms "state agency," "agency," "institution," "public body," and "public institution of higher education," shall not include the University of Virginia Medical Center.

"Technology asset" means hardware and communications equipment not classified as traditional mainframe-based items, including personal computers, mobile computers, and other devices capable of storing and manipulating electronic data.

"Telecommunications" means any origination, transmission, emission, or reception of data, signs, signals, writings, images, and sounds or intelligence of any nature, by wire, radio, television, optical, or other electromagnetic systems.

"Telecommunications facilities" means apparatus necessary or useful in the production, distribution, or interconnection of electronic communications for state agencies or institutions including the buildings and structures necessary to house such apparatus and the necessary land.

§ 2.2-2007. Powers of the CIO.

A. In addition to such other duties as the Secretary may assign, the CIO shall:

1. Monitor trends and advances in information technology; develop a comprehensive six-year Commonwealth strategic plan for information technology to include: (i) specific projects that implement the plan; (ii) a plan for the acquisition, management, and use of information technology by state agencies; (iii) a report of the progress of any ongoing enterprise information technology projects, any factors or risks that might affect their successful completion, and any changes to their projected implementation costs and schedules; and (iv) a report on the progress made by state agencies toward accomplishing the Commonwealth strategic plan for information technology. The Commonwealth strategic plan for information technology shall be updated annually and submitted to the Secretary for approval.

2. Direct the formulation and promulgation of policies, guidelines, standards, and specifications for the purchase, development, and maintenance of information technology for state agencies, including, but not limited to, those (i) required to support state and local government exchange, acquisition, storage,

use, sharing, and distribution of geographic or base map data and related technologies, (ii) concerned with the development of electronic transactions including the use of electronic signatures as provided in § 59.1-496, and (iii) necessary to support a unified approach to information technology across the totality of state government, thereby assuring that the citizens and businesses of the Commonwealth receive the greatest possible security, value, and convenience from investments made in technology.

3. Direct the development of policies and procedures, in consultation with the Department of Planning and Budget, that are integrated into the Commonwealth's strategic planning and performance budgeting processes, and that state agencies and public institutions of higher education shall follow in developing information technology plans and technology-related budget requests. Such policies and procedures shall require consideration of the contribution of current and proposed technology expenditures to the support of agency and institution priority functional activities, as well as current and future operating expenses, and shall be utilized by all state agencies and public institutions of higher education in preparing budget requests.

4. Review budget requests for information technology from state agencies and public institutions of higher education and recommend budget priorities to the Secretary.

Review of such budget requests shall include, but not be limited to, all data processing or other related projects for amounts exceeding $250,000 in which the agency or institution has entered into or plans to enter into a contract, agreement or other financing agreement or such other arrangement that requires that the Commonwealth either pay for the contract by foregoing revenue collections, or allows or assigns to another party the collection on behalf of or for the Commonwealth any fees, charges, or other assessments or revenues to pay for the project. For each project, the agency or institution, with the exception of public institutions of higher education that meet the conditions prescribed in subsection B of § 23-38.88, shall provide the CIO (i) a summary of the terms, (ii) the anticipated duration, and (iii) the cost or charges to any user, whether a state agency or institution or other party not directly a party to the project arrangements. The description shall also include any terms or conditions that bind the Commonwealth or restrict the Commonwealth's operations and the methods of procurement employed to reach such terms.

State agencies and institutions, with the exception of public institutions of higher education that meet the conditions prescribed in subsection B of § 23-38.88, shall submit to the CIO a projected biennial operations and maintenance budget for technology assets owned or licensed by the agency or institution, and submit a budget decision package for any shortfalls.

5. Direct the development of policies and procedures for the effective management of information technology investments throughout their entire life cycles, including, but not limited to, identification, business case development, selection, procurement, implementation, operation, performance evaluation, and enhancement or retirement. Such policies and procedures shall include, at a minimum, the periodic review by the CIO of agency and public institution of higher education Commonwealth information technology projects.

6. Provide technical guidance to the Department of General Services in the development of policies and procedures for the recycling and disposal of computers and other technology assets. Such policies and procedures shall include the expunging, in a manner as determined by the ~~CIO~~ *CISO*, of all state 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.

7. Oversee and administer the Virginia Technology Infrastructure Fund created pursuant to § 2.2-2023.

8. Periodically evaluate the feasibility of outsourcing information technology resources and services, and outsource those resources and services that are feasible and beneficial to the Commonwealth.

9. Have the authority to enter into contracts with one or more other public bodies, or public agencies or institutions or localities of the several states, of the United States or its territories, or the District of Columbia for the provision of information technology services.

10. Report annually to the Governor, the Secretary, and the Joint Commission on Technology and Science created pursuant to § 30-85 on the use and application of information technology by state agencies and public institutions of higher education to increase economic efficiency, citizen convenience, and public access to state government. The CIO shall prepare an annual report for submission to the Secretary, the Information Technology Advisory Council, and the Joint Commission on Technology and Science on a prioritized list of Recommended Technology Investment Projects (RTIP Report) based upon major information technology projects submitted for business case approval pursuant to this chapter. As part of the RTIP Report, the CIO shall develop and regularly update a methodology for prioritizing projects based upon the allocation of points to defined criteria. The criteria and their definitions shall be presented in the RTIP Report. For each project recommended for funding in the RTIP Report, the CIO shall indicate the number of points and how they were awarded. For each listed project, the CIO shall also report (i) all projected costs of ongoing operations and maintenance activities

of the project for the next three biennia following project implementation; (ii) a justification and description for each project baseline change; and (iii) whether the project fails to incorporate existing standards for the maintenance, exchange, and security of data. This report shall also include trends in current projected information technology spending by state agencies and secretariats, including spending on projects, operations and maintenance, and payments to VITA. Agencies shall provide all project and cost information required to complete the RTIP Report to the CIO prior to May 31 immediately preceding any budget biennium in which the project appears in the Governor's budget bill.

11. Direct the development of policies and procedures that require the Division of Project Management established pursuant to § 2.2-2016, on behalf of the CIO, to review and recommend Commonwealth information technology projects proposed by state agencies and institutions. Such policies and procedures shall be based on the criteria outlined within § 2.2-2017.

12. Provide oversight for state agency or public institution of higher education efforts to modernize the planning, development, implementation, improvement, operations and maintenance, and retirement of Commonwealth information technology, including oversight for the selection, development and management of enterprise information technology.

13. Develop statewide technical and data standards for information technology and related systems, including the utilization of nationally recognized technical and data standards for health information technology systems or software purchased by a state agency of the Commonwealth.

14. Establish Internal Agency Oversight Committees and Secretariat Oversight Committees as necessary and in accordance with § 2.2-2021.

B. Consistent with § 2.2-2012, the CIO may enter into public-private partnership contracts to finance or implement information technology programs and projects. The CIO may issue a request for information to seek out potential private partners interested in providing programs or projects pursuant to an agreement under this subsection. The compensation for such services shall be computed with reference to and paid from the increased revenue or cost savings attributable to the successful implementation of the program or project for the period specified in the contract. The CIO shall be responsible for reviewing and approving the programs and projects and the terms of contracts for same under this subsection. The CIO shall determine annually the total amount of increased revenue or cost savings attributable to the successful implementation of a program or project under this subsection and such amount shall be deposited in the Virginia Technology Infrastructure Fund created in § 2.2-2023. The CIO is authorized to use moneys deposited in the Fund to pay private partners pursuant to the terms of contracts under this subsection. All moneys in excess of that required to be paid to private partners, as determined by the CIO, shall be reported to the Comptroller and retained in the Fund. The CIO shall prepare an annual report to the Governor, the Secretary, and General Assembly on all contracts under this subsection, describing each information technology program or project, its progress, revenue impact, and such other information as may be relevant.

C. The CIO shall develop a technology investment management standard based on acceptable technology investment methods to ensure that all state agency or public institution of higher education technology expenditures are an integral part of the Commonwealth's performance management system, produce value for the agency and the Commonwealth, and are aligned with (i) agency strategic plans, (ii) the Governor's policy objectives, and (iii) the long-term objectives of the Council on Virginia's Future.

D. The CIO shall have the authority to enter into and amend contracts for the provision of information technology services.

§ 2.2-2009. Appointment of the CISO; duties of the CISO relating to security of government information and applications.

A. To provide for the security of state government electronic information from unauthorized uses, intrusions or other security threats, ~~the CIO~~ *the Governor shall appoint a Chief Information Security Officer of the Commonwealth (CISO) to oversee the security of government information and applications in the Commonwealth. The CISO shall be a full-time, classified employee and report to the CIO. The CISO shall exercise the powers and duties conferred or imposed upon him by this chapter and perform such other duties as may be required by the Governor and the Secretary of Technology.*

B. The CISO shall direct the development of policies, procedures, and standards for assessing security risks, determining the appropriate security measures, and performing security audits of government electronic information *and applications*. Such policies, procedures, and standards ~~will~~ *shall* apply to the Commonwealth's executive, legislative, and judicial branches~~, and~~*;* independent agencies*;* and institutions of higher education. The ~~CIO~~ *CISO* shall work with representatives of the Chief Justice of the Supreme Court and Joint Rules Committee of the General Assembly to identify their needs.

~~B.~~ *C.* The ~~CIO~~ *CISO* shall also develop policies, procedures, and standards that shall address the scope of security audits and the frequency of such security audits. In developing and updating such policies, procedures, and standards, the ~~CIO~~ *CISO* shall ~~designate a government entity to~~ oversee, plan, and coordinate the conduct of periodic security audits of all executive branch and independent agencies

and institutions of higher education. The ~~CIO~~ ~~will~~ *CISO 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.

~~C.~~ *D.* The ~~CIO~~ *CISO* shall annually report to the Governor, the Secretary, and General Assembly *the results of security audits, including the extent to which security standards and guidelines have been adopted by state agencies, as well as* those executive branch and independent agencies and institutions of higher education that have not implemented acceptable policies, procedures, and standards to control unauthorized uses, intrusions, or other security threats. For any executive branch or independent agency or institution of higher education whose security audit results and plans for corrective action are unacceptable, the ~~CIO~~ *CISO* 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~~ *CISO* may *recommend that the CIO (a)* take action to suspend the public body's information technology projects pursuant to § 2.2-2015~~,~~ *or (b)* limit additional information technology investments pending acceptable corrective actions~~, and~~. *The CISO may* recommend to the Governor and Secretary any other appropriate actions.

~~The CIO shall also include in this report (a) results of security audits, including those state agencies, independent agencies, and institutions of higher education that have not implemented acceptable regulations, standards, policies, and guidelines to control unauthorized uses, intrusions, or other security threats and (b) the extent to which security standards and guidelines have been adopted by state agencies.~~

~~D.~~ *E.* All public bodies subject to such audits as required by this section shall fully cooperate with the ~~entity designated to perform such audits~~ *CISO* and bear any associated costs. Public bodies that are not required to but elect to use the ~~entity designated~~ *CISO* to perform such audits shall also bear any associated costs.

~~E.~~ *F.* 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.

~~F.~~ *G.* To ensure the security and privacy of citizens of the Commonwealth in their interactions with state government, the ~~CIO~~ *CISO* shall direct the development of policies, procedures, and standards for the protection of confidential data maintained by state agencies against unauthorized access and use. Such policies, procedures, and standards shall include, but not be limited to:

1. Requirements that any state employee or other authorized user of a state technology asset provide passwords or other means of authentication to (i) use a technology asset and (ii) access a state-owned or operated computer network or database; and

2. Requirements that 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 data to authorized individuals.

~~G.~~ *H.* The ~~CIO~~ *CISO* 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.

~~H.~~ *I.* The ~~CIO~~ *CISO* shall also develop policies, procedures, and standards that shall 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~~ *CISO*. Such cooperation includes, but is not limited to, (i) providing the ~~CIO~~ *CISO* 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.

~~I.~~ *J.* The ~~CIO~~ *CISO* 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, procedures, and standards developed pursuant to this section.