

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.

INTRODUCED

HB509

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

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

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

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

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

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

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

80 "Noncommercial telecommunications entity" means any public broadcasting station as defined in
81 § 22.1-20.1.

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

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

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

92 "Public telecommunications services" means public broadcasting services.

93 "Secretary" means the Secretary of Technology.

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

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

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

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

107 **§ 2.2-2007. Powers of the CIO.**

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

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

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

121 use, sharing, and distribution of geographic or base map data and related technologies, (ii) concerned
122 with the development of electronic transactions including the use of electronic signatures as provided in
123 § 59.1-496, and (iii) necessary to support a unified approach to information technology across the
124 totality of state government, thereby assuring that the citizens and businesses of the Commonwealth
125 receive the greatest possible security, value, and convenience from investments made in technology.

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

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

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

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

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

158 6. Provide technical guidance to the Department of General Services in the development of policies
159 and procedures for the recycling and disposal of computers and other technology assets. Such policies
160 and procedures shall include the expunging, in a manner as determined by the CIO CISO, of all state
161 confidential data and personal identifying information of citizens of the Commonwealth prior to such
162 sale, disposal, or other transfer of computers or other technology assets.

163 7. Oversee and administer the Virginia Technology Infrastructure Fund created pursuant to
164 § 2.2-2023.

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

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

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

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

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

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

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

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

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

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

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

226 **§ 2.2-2009. Appointment of the CISO; duties of the CISO relating to security of government**
 227 **information and applications.**

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

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

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

244 and institutions of higher education. The ~~CEO~~ *CISO shall* coordinate these audits with the Auditor
245 of Public Accounts and the Joint Legislative Audit and Review Commission. The Chief Justice of the
246 Supreme Court and the Joint Rules Committee of the General Assembly shall determine the most
247 appropriate methods to review the protection of electronic information within their branches.

248 ~~C. D.~~ The ~~CEO~~ *CISO shall* annually report to the Governor, the Secretary, and General Assembly *the*
249 *results of security audits, including the extent to which security standards and guidelines have been*
250 *adopted by state agencies, as well as those executive branch and independent agencies and institutions*
251 *of higher education that have not implemented acceptable policies, procedures, and standards to control*
252 *unauthorized uses, intrusions, or other security threats. For any executive branch or independent agency*
253 *or institution of higher education whose security audit results and plans for corrective action are*
254 *unacceptable, the ~~CEO~~ CISO shall report such results to (i) the Secretary, (ii) any other affected cabinet*
255 *secretary, (iii) the Governor, and (iv) the Auditor of Public Accounts. Upon review of the security audit*
256 *results in question, the ~~CEO~~ CISO may recommend that the CIO (a) take action to suspend the public*
257 *body's information technology projects pursuant to § 2.2-2015; or (b) limit additional information*
258 *technology investments pending acceptable corrective actions; and. The CISO may recommend to the*
259 *Governor and Secretary any other appropriate actions.*

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

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

269 ~~E. F.~~ The provisions of this section shall not infringe upon responsibilities assigned to the
270 Comptroller, the Auditor of Public Accounts, or the Joint Legislative Audit and Review Commission by
271 other provisions of the Code of Virginia.

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

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

279 2. Requirements that a digital rights management system or other means of authenticating and
280 controlling an individual's ability to access electronic records be utilized to limit access to and use of
281 electronic records that contain confidential data to authorized individuals.

282 ~~G. H.~~ The ~~CEO~~ *CISO shall* promptly receive reports from directors of departments in the executive
283 branch of state government made in accordance with § 2.2-603 and shall take such actions as are
284 necessary, convenient or desirable to ensure the security of the Commonwealth's electronic information
285 and confidential data.

286 ~~H. I.~~ The ~~CEO~~ *CISO shall* also develop policies, procedures, and standards that shall address the
287 creation and operation of a risk management program designed to identify information technology
288 security gaps and develop plans to mitigate the gaps. All agencies in the Commonwealth shall cooperate
289 with the ~~CEO~~ *CISO*. Such cooperation includes, but is not limited to, (i) providing the ~~CEO~~ *CISO* with
290 information required to create and implement a Commonwealth risk management program; (ii) creating
291 an agency risk management program; and (iii) complying with all other risk management activities.

292 ~~I. J.~~ The ~~CEO~~ *CISO shall* provide all directors of agencies and departments with all such information,
293 guidance, and assistance required to ensure that agencies and departments understand and adhere to the
294 policies, procedures, and standards developed pursuant to this section.