050079784

SENATE BILL NO. 1252

AMENDMENT IN THE NATURE OF A SUBSTITUTE

(Proposed by the Senate Committee on General Laws

on January 26, 2005)

(Patron Prior to Substitute—Senator O'Brien)

A BILL to amend and reenact §§ 2.2-603 and 2.2-2009 of the Code of Virginia, relating to security of government databases.

Be it enacted by the General Assembly of Virginia:

1. That §§ 2.2-603 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. [Repealed.]

G. *Notwithstanding subsection D,* the director of every department in the executive branch of state government *and public institutions of higher education* shall report to the Chief Information Officer *(CIO)* as described in § 2.2-2005, 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 *or institution* activities. Such reports shall be made to the ~~Chief Information Officer~~ *CIO* within 24 hours from when the department *or institution* discovered or should have discovered their occurrence. *The CIO shall include such reports in the annual security audits conducted pursuant to § 2.2-2009.*

§ 2.2-2009. Additional duties of the CIO relating to security of government databases and data communications.

A. To ensure the security of state government databases and data communications from unauthorized uses, intrusions or other security threats, the CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government databases and data communications. At a minimum, these policies, procedures and standards shall address the scope of security audits and which public bodies are authorized to conduct security audits. In developing and updating such policies, procedures and standards, the CIO shall consider, at a minimum, the advice and recommendations of the Council on Technology Services created pursuant to § 2.2-2651.

B. The CIO shall ~~designate a government entity to~~ oversee, plan, and coordinate the conduct of ~~periodic~~ *annual* security audits of all ~~executive branch~~ agencies and *public* institutions of higher education regarding the protection of government databases and data communications.

1. Security audits may include, but are not limited to, on-site audits as well as reviews of all written

security procedures.

2. The ~~designated entity~~ *CIO* may contract with ~~a private firm or firms~~ *any entity* that ~~specialize~~ *specializes* in conducting such audits ~~subject to approval of the CIO~~.

C. All ~~public bodies~~ *agencies and institutions* subject to ~~such~~ audits ~~as~~ required by this section shall fully cooperate ~~with~~ *in* the ~~entity designated to perform~~ *conduct of* such audits.

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. (Effective January 1, 2005)~~ The CIO shall promptly receive reports from directors of departments in the executive branch of state government *and public institutions of higher education* 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 databases and data communications. *The CIO shall include these reports in the annual security audit of the agency or institution.*

F. The CIO shall have the authority to assist and monitor any remediation that may be required to mitigate any risks or vulnerabilities discovered by audits. Any remediation may be delayed if a law-enforcement agency determines that such remediation will impede a criminal investigation.

G. By December 1 of every year, the CIO shall report a summary of the results of the audits conducted pursuant to this section to the Governor, the General Assembly, and the Joint Commission on Technology and Science.

H. 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.