VIRGINIA ACTS OF ASSEMBLY -- 2007 SESSION

CHAPTER 775

An Act to amend and reenact § 2.2-2009 of the Code of Virginia, relating to the security of government information.

[S 1029]

Approved March 23, 2007

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 ~~ensure~~ *provide for* the security of state government ~~databases and data communications~~ *electronic information* 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~~ *electronic information*. ~~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.~~ *Such policies, procedures, and standards will apply to the Commonwealth's executive, legislative, and judicial branches, and independent agencies and institutions of higher education. 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.*

B. The CIO 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 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. ~~regarding the protection of government databases and data communications.~~ *The CIO will 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.*

~~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 may contract with a private firm or firms that specialize in conducting such audits subject to approval of the CIO.~~

C. *The CIO shall report to the Governor and General Assembly by December 2008 and annually thereafter, 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 and independent agency or institution of higher education whose security audit results and plans for corrective action are unacceptable, the CIO shall report such results to the (i) Information Technology Investment Board, (ii) affected cabinet secretary, (iii) Governor, and (iv) Auditor of Public Accounts. Upon review of the security audit results in question, the Information Technology Investment Board may take action to suspend the public bodies information technology projects pursuant to subdivision 3 of § 2.2-2458, limit additional information technology investments pending acceptable corrective actions, and recommend to the Governor any other appropriate actions.*

D. All public bodies 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*.

~~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 ~~databases and data communications~~ *electronic information*.