COMMITTEE SUBSTITUTE

FOR

Senate Bill No. 630

(By Senator Unger)

_____

[Originating in the Committee on Government Organization;

reported March 28, 2013.]

_____

A BILL to amend and reenact §5A-6-4a of the Code of West Virginia, 1931, as amended, relating to duties of the Chief Technology Officer with regard to security of government information; adding the Division of Protective Services and the West Virginia Intelligence Fusion Center to the list of agencies exempted from the control of the Chief Technology Officer; and adding the Treasurer to the list of officers whose responsibilities cannot be infringed upon by the Chief Technology Officer.

Be it enacted by the Legislature of West Virginia:

That §5A-6-4a of the Code of West Virginia, 1931, as amended, be amended and reenacted to read as follows:

ARTICLE 6. OFFICE OF TECHNOLOGY.

§5A-6-4a. Duties of the Chief Technology Officer relating to security of government information.

(a) To ensure the security of state government information and

the data communications infrastructure from unauthorized uses, intrusions or other security threats, the Chief Technology Officer is authorized to develop policies, procedures, standards and legislative rules. At a minimum, these policies, procedures and standards shall identify and require the adoption of practices to safeguard information systems, data and communications infrastructures, as well as define the scope and regularity of security audits and which bodies are authorized to conduct security audits. The audits may include reviews of physical security practices.

(b) (1) The Chief Technology Officer shall at least annually perform security audits of all executive branch agencies regarding the protection of government databases and data communications.

(2) Security audits may include, but are not limited to, on-site audits as well as reviews of all written security procedures and documented practices.

(c) The Chief Technology Officer may contract with a private firm or firms that specialize in conducting these audits.

(d) All public bodies subject to the audits required by this section shall fully cooperate with the entity designated to perform the audit.

(e) The Chief Technology Officer may direct specific remediation actions to mitigate findings of insufficient administrative, technical and physical controls necessary to protect state government information or data communication infrastructures.

(f) The Chief Technology Officer shall ~~promulgate legislative~~ propose rules for legislative approval in accordance with the provisions of chapter twenty-nine-a of this code, to minimize vulnerability to threats and to regularly assess security risks, determine appropriate security measures and perform security audits of government information systems and data communications infrastructures.

(g) To ensure compliance with confidentiality restrictions and other security guidelines applicable to state law-enforcement agencies, emergency response personnel and emergency management operations, the provisions of this section ~~may~~ do not apply to the West Virginia State Police, ~~or~~ the Division of Protective Services, the West Virginia Intelligence Fusion Center or the Division of Homeland Security and Emergency Management.

(h) The provisions of this section ~~shall~~ do not infringe upon the responsibilities assigned to the state Comptroller, the Treasurer, the Auditor or the Legislative Auditor, or other statutory requirements.

(i) In consultation with the Adjutant General, Chairman of the Public Service Commission, the Superintendent of the State Police and the Director of the Division of Homeland Security and Emergency Management, the Chief Technology Officer is responsible for the development and maintenance of an information systems disaster recovery system for the State of West Virginia with redundant sites in two or more locations isolated from reasonably perceived threats to the primary operation of state government. The Chief Technology

Officer shall develop specifications, funding mechanisms and participation requirements for all executive branch agencies to protect the state's essential data, information systems and critical government services in times of emergency, inoperativeness or disaster. Each executive branch agency shall assist the Chief Technology Officer in planning for its specific needs and provide to the Chief Technology Officer any information or access to information systems or equipment that may be required in carrying out this purpose. No statewide or executive branch agency procurement of disaster recovery services may be initiated, let or extended without the expressed consent of the Chief Technology Officer.