

**WEST VIRGINIA LEGISLATURE**  
**EIGHTY-FIRST LEGISLATURE**  
**REGULAR SESSION, 2013**



**ENROLLED**

COMMITTEE SUBSTITUTE

FOR

**Senate Bill No. 630**

(SENATOR UNGER, *ORIGINAL SPONSOR*)

[PASSED APRIL 13, 2013; IN EFFECT FROM PASSAGE.]

**E N R O L L E D**

COMMITTEE SUBSTITUTE

FOR

**Senate Bill No. 630**

(SENATOR UNGER, *original sponsor*)

---

[Passed April 13, 2013; in effect from passage.]

---

AN ACT 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.**

1 (a) To ensure the security of state government  
2 information and the data communications infrastructure from  
3 unauthorized uses, intrusions or other security threats, the  
4 Chief Technology Officer is authorized to develop policies,  
5 procedures, standards and legislative rules. At a minimum,  
6 these policies, procedures and standards shall identify and  
7 require the adoption of practices to safeguard information  
8 systems, data and communications infrastructures, as well as  
9 define the scope and regularity of security audits and which  
10 bodies are authorized to conduct security audits. The audits  
11 may include reviews of physical security practices.

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

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

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

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

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

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

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

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

49 (i) In consultation with the Adjutant General, Chairman  
50 of the Public Service Commission, the Superintendent of the  
51 State Police and the Director of the Division of Homeland  
52 Security and Emergency Management, the Chief Technology  
53 Officer is responsible for the development and maintenance  
54 of an information systems disaster recovery system for the  
55 State of West Virginia with redundant sites in two or more  
56 locations isolated from reasonably perceived threats to the  
57 primary operation of state government. The Chief  
58 Technology Officer shall develop specifications, funding  
59 mechanisms and participation requirements for all executive  
60 branch agencies to protect the state's essential data,  
61 information systems and critical government services in

62 times of emergency, inoperativeness or disaster. Each  
63 executive branch agency shall assist the Chief Technology  
64 Officer in planning for its specific needs and provide to the  
65 Chief Technology Officer any information or access to  
66 information systems or equipment that may be required in  
67 carrying out this purpose. No statewide or executive branch  
68 agency procurement of disaster recovery services may be  
69 initiated, let or extended without the expressed consent of the  
70 Chief Technology Officer.

The Joint Committee on Enrolled Bills hereby certifies that the foregoing bill is correctly enrolled.

.....  
*Chairman Senate Committee*

.....  
*Chairman House Committee*

Originated in the Senate.

In effect from passage.

.....  
*Clerk of the Senate*

.....  
*Clerk of the House of Delegates*

.....  
*President of the Senate*

.....  
*Speaker of the House of Delegates*

\_\_\_\_\_

The within ..... this the .....

Day of ....., 2013.

.....  
*Governor*