

WEST VIRGINIA LEGISLATURE

2019 REGULAR SESSION

Committee Substitute

for

House Bill 2452

BY MR. SPEAKER (MR. HANSHAW) AND DELEGATE MILEY

[BY REQUEST OF THE EXECUTIVE]

[Originating in the Committee on Finance, February

19, 2019.]

1 A BILL to repeal §5A-6-4a of the Code of West Virginia, 1931, as amended; and to amend said
2 code by adding thereto a new article, designated §5A-6B-1, §5A-6B-2, §5A-6B-3, §5A-
3 6B-4, §5A-6B-5 and §5A-6B-6, all relating to cybersecurity of state government; removing
4 the requirements of the Chief Technology Officer to oversee security of government
5 information; creating the Cybersecurity Office; defining terms; providing that the Chief
6 Information Security Officer to oversee the Cybersecurity Office; authorizing the Chief
7 Information Security Officer to create a cybersecurity framework, to assist and provide
8 guidance to agencies in cyber risk strategy and setting forth other duties; providing rule-
9 making authority; requiring agencies to undergo cyber risk assessments; establishing
10 scope of authority; exempting certain state entities; designating reporting requirements;
11 requiring agencies to address any cybersecurity deficiencies; exempting information
12 related to cyber risk from public disclosure; and requiring annual reports to the Joint
13 Committee on Government and Finance and to the Governor on the status of the
14 cybersecurity program, including any recommended statutory changes.

Be it enacted by the Legislature of West Virginia:

ARTICLE 6. OFFICE OF TECHNOLOGY.

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

1 [Repealed.]

ARTICLE 6B. CYBER SECURITY PROGRAM.

§5A-6B-1. West Virginia Cybersecurity Office; scope; exemptions.

1 (a) There is hereby created the West Virginia Cybersecurity Office within the Office of
2 Technology. The office has the authority to set standards for cybersecurity and is charged with
3 managing the cybersecurity framework.

4 (b) The provisions of this article are applicable to all state agencies, excluding higher
5 education institutions, the State Police, state constitutional officers identified in §6-7-2 of this code,
6 the Legislature and the Judiciary.

§5A-6B-2. Definitions.

1 As used in this article:

2 “Cybersecurity framework” means computer technology security guidance for
3 organizations to assess and improve their ability to prevent, detect, and respond to cyber
4 incidents.

5 “Cyber incident” means any event that threatens the security, confidentiality, integrity, or
6 availability of information assets, information systems, or the networks that deliver the information.

7 “Cyber risk assessment” means the process of identifying, analyzing and evaluating risk
8 and applying the appropriate security controls relevant to the information custodians.

9 “Cyber risk management service” means technologies, practices and policies that address
10 threats and vulnerabilities in networks, computers, programs and data, flowing from or enabled
11 by connection to digital infrastructure, information systems or industrial control systems, including,
12 but not limited to, information security, supply chain assurance, information assistance and
13 hardware or software assurance.

14 “Enterprise” means the collective departments, agencies and boards within state
15 government that provide services to citizens and other state entities.

16 “Information custodian” means a department, agency or person that has the actual
17 custody of, or is responsible for the accountability for a set of data assets.

18 “Plan of action and milestones” means a remedial plan, or the process of accepting or
19 resolving risk, which helps the information custodian to identify and assess information system
20 security and privacy weaknesses, set priorities and monitor progress toward mitigating the
21 weaknesses.

22 “Privacy impact assessment” means a procedure or tool for identifying and assessing
23 privacy risks throughout the development life cycle of a program or system.

24 “Security controls” means safeguards or countermeasures to avoid, detect, counteract or
25 minimize security risks to physical property, information, computer systems or other assets.

§5A-6B-3. Powers and duties of Chief Information Security Officer; staff; rule-making.

1 (a) The West Virginia Cybersecurity Office is under the supervision and control of a Chief
2 Information Security Officer appointed by the Chief Technology Officer and shall be staffed
3 appropriately by the Office of Technology to implement the provisions of this article.

4 (b) The Chief Information Security Officer has the following powers and duties:

5 (1) Develop policies, procedures and standards necessary to establish an enterprise
6 cybersecurity program that recognizes the interdependent relationship and complexity of
7 technology in government operations and the nature of shared risk of cyber threats to the state;

8 (2) Create a cyber risk management service designed to ensure that officials at all levels
9 understand their responsibilities for managing their agencies’ cyber risk;

10 (3) Designate a cyber risk standard for the cybersecurity framework;

11 (4) Establish the cyber risk assessment requirements such as assessment type, scope,
12 frequency and reporting;

13 (5) Provide agencies cyber risk guidance for information technology projects, including the
14 recommendation of security controls and remediation plans;

15 (6) Assist agencies in the development of plans and procedures to manage, assist and
16 recover in the event of a cyber incident;

17 (7) Assist agencies in the management of the framework relating to information custody,
18 classification, accountability and protection;

19 (8) Ensure uniformity and adequacy of the cyber risk assessments;

20 (9) Notwithstanding the provisions of §5A-6B-1(b) of this code, enter into agreements with
21 state government entities exempted from the application of this article or other political

22 subdivisions of the state that desire to voluntarily participate in the cybersecurity program
23 administered pursuant to this article;

24 (10) Develop policy outlining use of the privacy impact assessment as it relates to
25 safeguarding of data and its relationship with technology; and

26 (11) Perform such other functions and duties as provided by law and as directed by the
27 Chief Technology Officer.

28 (c) The Secretary of the Department of Administration shall propose rules for legislative
29 approval in accordance with §29A-3-1 et seq. of this code to implement and enforce the provisions
30 of this article.

§5A-6B-4. Responsibilities of agencies for cybersecurity.

1 State agencies and other entities subject to the provisions of this article shall:

2 (1) Undergo an appropriate cyber risk assessment as required by the cybersecurity
3 framework or as directed by the Chief Information Security Officer;

4 (2) Adhere to the cybersecurity standard established by the Chief Information Security
5 Officer in the use of information technology infrastructure;

6 (3) Adhere to enterprise cybersecurity policies and standards;

7 (4) Manage cybersecurity policies and procedures where more restricted security controls
8 are deemed appropriate;

9 (5) Submit all cybersecurity policy and standard exception requests to the Chief
10 Information Security Officer for approval;

11 (6) Complete and submit a cyber risk self-assessment report to the Chief Information
12 Security Officer by December 31, 2020; and

13 (7) Manage a plan of action and milestones based on the findings of the cyber risk
14 assessment and business needs.

§5A-6B-5. Exemption from disclosure.

1 Any information, including, but not limited to, cyber risk assessments, plans of action and
2 milestones, remediation plans, or information indicating the cyber threat, vulnerability, information
3 or data that may identify or expose potential impacts or risk to agencies or to the state or that
4 could threaten the technology infrastructure critical to government operations and services, public
5 safety or health is exempt from §29B-1-1 et seq. of this code.

§5A-6B-6. Annual reports.

1 The Chief Information Security Officer shall annually, beginning on December 1, 2019,
2 and on December 1 of each year thereafter, report to the Joint Committee on Government and
3 Finance and to the Governor on the status of the cybersecurity program, including any
4 recommended statutory changes.