

WEST VIRGINIA LEGISLATURE

2026 REGULAR SESSION

ENGROSSED

House Bill 5638

By Delegate Linville

[By Request of the Department of Administration]

[Introduced February 17, 2026; referred
to the Committee on Energy and Public Works]

1 A BILL to amend and reenact §5A-6B-1, §5A-6B-2, §5A-6B-3, §5A-6B-4, §5A-6B-5, and §5A-6B-6
2 of the Code of West Virginia, 1931, as amended, relating to the requirements of the states
3 cyber security program and responsibilities and authority of the state Chief Information
4 Security Officer.

5 *Be it enacted by the Legislature of West Virginia:*

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, to be led by the West Virginia Chief Information Security Officer. The office ~~has the~~
3 ~~authority to~~ may set standards for cybersecurity and is charged with managing the cybersecurity
4 framework.

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

8 **§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~~ Cybersecurity program review" means the process of identifying,
8 analyzing and evaluating risk and applying the appropriate security controls relevant to the
9 information custodian.

10 "Cyber risk management service" means technologies, practices and policies that address
11 threats and vulnerabilities in networks, computers, programs, and data flowing from or enabled by

12 connection to digital infrastructure, information systems, networks, devices, or industrial control
13 systems, including, but not limited to, information security, supply chain assurance, information
14 assistance and hardware or software assurance.

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

17 "Framework" means cybersecurity framework as defined in this section.

18 "Incident" means cyber incident as defined in this section.

19 "Information custodian" means a state or local department, agency, ~~or person that has the~~
20 ~~actual custody of, or is responsible for the accountability for a set of~~ office, board, commission, or
21 other spending unit with custody of, or responsibility for, data assets residing on a state system,
22 device, account or network. Networks owned, monitored, or maintained by the West Virginia Office
23 of Technology.

24 "Plan of action and milestones" means a remedial plan, or the process of accepting or
25 resolving risk, which helps the information custodian to identify and assess information system
26 security and privacy weaknesses, set priorities and monitor progress toward mitigating the
27 weaknesses.

28 "Privacy impact assessment" means a procedure or tool for identifying and assessing
29 privacy risks throughout the development life cycle of a program or system.

30 "Security controls" means safeguards or countermeasures to avoid, detect, counteract or
31 minimize security risks to physical property, information, computer systems or other assets.

32 "User" means an entity or person with access to a state system, device, account or
33 network. This includes, but is not limited to, employees, contractors, vendors, automated systems,
34 service accounts, and volunteers.

§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~~ Information Officer and shall be
3 staffed 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~~ may:

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 based on federal and industry best practices and
11 accepted principles for the cybersecurity framework;

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

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

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

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

20 (8) Ensure a minimum standard for uniformity and adequacy of the cyber risk
21 assessments;

22 (9) Notwithstanding the provisions of §5A-6B-1(b) of this code, enter into fee based
23 agreements with state government entities exempted from the application of this article or other
24 political subdivisions of the state that desire to voluntarily participate in the cybersecurity program
25 administered pursuant to this article;

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

28 (11) Establish minimal training requirements for users of state networks, systems, or
29 devices.

30 (12) Perform such other functions and duties as provided by law and as or directed by the
31 Chief ~~Technology~~ Information Officer.

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

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

1 ~~State agencies and other entities~~ (a) Each information custodian receiving centralized
2 support from the West Virginia Office of Technology, or any other entity subject to the provisions of
3 this article, shall:

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

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

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

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

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

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

15 ~~(7) Manage a plan of action and milestones based on the findings of the cyber risk~~
16 ~~assessment and business needs; and~~

17 ~~(8) Submit annual reports to the Chief Security Information Officer no later than November~~
18 ~~1 of each year beginning on November 1, 2023. The report shall contain an~~

19 (6) Participate in at least one annual cybersecurity program review with representatives of
20 the West Virginia Office of Technology before November 30 of each year. The review will provide
21 the Office of Technology with an analysis and evaluation of each ~~agency or entity's~~ information
22 custodian's cybersecurity readiness, ability to keep user data safe, data classifications, and other
23 steps that the ~~agency, or entity~~ information custodian has taken towards safeguarding, risk
24 management, cybersecurity readiness, or information technology modernization. ~~that are~~
25 ~~consistent with the objectives of §5A-6-4d and §5A-6-4e of this code~~

26 (A) If an information custodian fails to participate in the annual cybersecurity program
27 review, the West Virginia Office of Technology may recover expenses associated with conducting
28 any diagnostics or evaluations performed to assure safety of the network, devices, and systems.
29 The amount charged to the information custodian may not exceed the actual costs incurred by the
30 West Virginia Office of Technology in performing the review, resolving identified problems, and
31 ensuring network security, protection, and continuity of operations.

32 **§5A-6B-5. Exemption from disclosure.**

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

§5A-6B-6. Annual reports.

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

4 statutory changes. The report shall include a comprehensive summary of ~~each state agency's~~
5 ~~report submitted~~ the annual cybersecurity program reviews completed pursuant to §5A-6B-4 of
6 this code regarding the ~~agency's~~ information custodian's cybersecurity readiness and the
7 ~~agency's~~ a list of information technology modernization efforts taken by the West Virginia Office of
8 Technology.