

WEST VIRGINIA LEGISLATURE

2026 REGULAR SESSION

ENROLLED

House Bill 5638

BY DELEGATE LINVILLE

(BY REQUEST OF THE DEPARTMENT OF ADMINISTRATION)

[Passed March 14, 2026; in effect 90 days from
passage (June 12, 2026)]

OFFICE OF WEST VIRGINIA
SECRETARY OF STATE

2026 APR - 1 P 10:56

FILED

HB 5638

WEST VIRGINIA LEGISLATURE

2026 REGULAR SESSION

ENROLLED

House Bill 5638

BY DELEGATE LINVILLE

(BY REQUEST OF THE DEPARTMENT OF ADMINISTRATION)

[Passed March 14, 2026; in effect 90 days from
passage (June 12, 2026)]

FILED
2025 APR -1 P 10:56
OFFICE OF THE CLERK
SECRETARY OF STATE

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

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 may set
3 standards for cybersecurity and is charged with 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 "Cybersecurity program review" means the process of identifying, analyzing and
8 evaluating risk, and applying the appropriate security controls relevant to the information
9 custodian.

10 "Cyber risk management service" means technologies, practices, and policies that
11 address threats and vulnerabilities in networks, computers, programs, and data flowing from or
12 enabled by connection to digital infrastructure, information systems, networks, devices, or

13 industrial control systems, including, but not limited to, information security, supply chain
14 assurance, information 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, office, board,
20 commission, or other spending unit with custody of, or responsibility for, data assets residing on
21 a state system, device, account, or networks owned, monitored, or maintained by the West
22 Virginia Office of Technology.

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

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

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

31 "User" means an entity or person with access to a state system, device, account, or
32 network. This includes, but is not limited to, employees, contractors, vendors, automated systems,
33 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 Information 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 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;

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

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

(c) The Chief Information Security Officer, along with the Chief Information Officer, shall ensure that any state contract for licensing software applications, which are designed to run on generally available desktop or server hardware, shall not limit the state's ability to install or run the software on the hardware of the state's choosing.

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

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

(a) Each information custodian receiving centralized support from the West Virginia Office of Technology, or any other entity subject to the provisions of this article, shall:

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

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

(3) Adhere to enterprise cybersecurity policies and standards;

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

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

(6) Participate in at least one annual cybersecurity program review with representatives of the West Virginia Office of Technology before November 30 of each year. The review will provide the Office of Technology with an analysis and evaluation of each information custodian's cybersecurity readiness, ability to keep user data safe, data classifications, and other steps that

16 the information custodian has taken towards safeguarding, risk management, cybersecurity
17 readiness, or information technology modernization.

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

§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
4 risk to agencies or to the state or that could threaten the technology infrastructure critical to
5 government operations 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, on December 1 of each year report
2 to the Joint Committee on Government and Finance and to the Governor on the status of the
3 cybersecurity program, including any recommended statutory changes. The report shall include
4 a comprehensive summary of the annual cybersecurity program reviews completed pursuant to
5 §5A-6B-4 of this code regarding the information custodian's cybersecurity readiness and a list of
6 information technology modernization efforts taken by the West Virginia Office of Technology.

The Clerk of the House of Delegates and the Clerk of the Senate hereby certify that the foregoing bill is correctly enrolled.


.....
Clerk of the House of Delegates

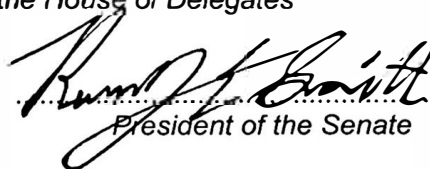

.....
Clerk of the Senate

FILED
2020 APR -1 P 10:55
OFFICE OF THE CLERK OF THE SENATE

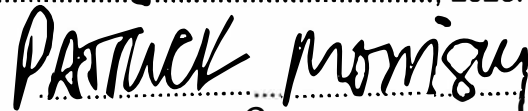
Originated in the House of Delegates.

In effect 90 days from passage.


.....
Speaker of the House of Delegates


.....
President of the Senate

The within is approved this the 1st
Day of April, 2026.


.....
Governor

PRESENTED TO THE GOVERNOR

11-11-2013

Time 3:30pm