WEST VIRGINIA LEGISLATURE

2026 REGULAR SESSION

Introduced

House Bill 5638

By Delegate Linville

[By Request of the Department of Administration]

[Introduced ; referred

to the Committee on the]

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 of the Code of West Virginia, 1931, as amended, relating to the requirements of the states cyber security program and responsibilities and authority of the state chief 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.

(a) There is hereby created the West Virginia Cybersecurity Office within the Office of Technology, to be led by the West Virginia Chief Information Security Officer. The office ~~has the authority to~~ may set standards for cybersecurity and is charged with managing the cybersecurity framework.

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

§5A-6B-2. Definitions.

As used in this article:

"Cybersecurity framework" means computer technology security guidance for organizations

to assess and improve their ability to prevent, detect, and respond to cyber incidents.

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

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

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

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

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

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

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

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

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

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

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

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

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

(a) The West Virginia Cybersecurity Office is under the supervision and control of a Chief Information Security Officer appointed by the Chief ~~Technology~~ Information Officer and shall be

staffed appropriately by the Office of Technology to implement the provisions of this article.

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

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

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

(3) Designate a cyber risk standard based on federal and industry best practices and accepted principles for the cybersecurity framework;

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

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

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

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

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

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

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

(11) Establish minimal training requirements for users of state networks, systems, or

devices.

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

(c) 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 ~~of agencies~~ for cybersecurity**.

~~State agencies and other entities~~ (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) Complete and submit a cyber risk self-assessment report to the Chief Information Security Officer by December 31, 2020;~~

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

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

(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 ~~agency or entity's~~ information custodian's cybersecurity readiness, ability to keep user data safe, data classifications, and other ste~~p~~s that the ~~agency, or entity~~ information custodian has taken towards safeguarding, risk management, cybersecurity readiness, or information technology modernization. ~~that are consistent with the objectives of §5A-6-4d and §5A-6-4e of this code~~

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

§5A-6B-5. Exemption from disclosure.

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

§5A-6B-6. Annual reports.

The Chief Information Security Officer shall annually, ~~beginning on December 1, 2019, and~~ on December 1 of each year ~~thereafter~~ report to the Joint Committee on Government and Finance and to the Governor on the status of the cybersecurity program, including any recommended statutory changes. The report shall include a comprehensive summary of ~~each state agency's report submitted~~ the annual cybersecurity program reviews completed pursuant to §5A-6B-4 of

this code regarding the ~~agency's~~ information custodian's cybersecurity readiness and ~~the~~ ~~agency's~~ a list of information technology modernization efforts taken by the West Virginia Office of Technology.

NOTE: The purpose of this bill is to clarify the authority and responsibilities of the state chief information security officer and outline the process for cybersecurity program reviews.

Strike-throughs indicate language that would be stricken from a heading or the present law and underscoring indicates new language that would be added.