WEST VIRGINIA LEGISLATURE

2019 REGULAR SESSION

Introduced

House Bill 2452

FISCAL NOTE

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

BY REQUEST OF THE EXECUTIVE

[Introduced January 16, 2019; Referred

to the Committee on Technology and Infrastructure

then Government Organization.]

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

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.

[Repealed.]

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. The office has the authority to 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 county boards of education, 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" means the process of identifying, analyzing and evaluating risk and applying the appropriate security controls relevant to the information custodians.

"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 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.

"Information custodian" means a department, agency or person who owns accountability for a set of data assets.

"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 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.

§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 Officer and shall be staffed appropriately to implement the provisions of this article.

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

(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 officials at all levels understand their responsibilities for managing their agencies' cyber risk;

(3) Designate a cyber risk standard 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 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 uniformity and adequacy of the cyber risk assessments;

(9) Enter into agreements with state government entities exempted from the application of this article to voluntarily participate in the cybersecurity program;

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

(11) Perform such other functions and duties as provided by law and as directed by the Chief Technology 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 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; and

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

§5A-6B-5. Exemption from disclosure.

Any information such as cyber risk assessments, plans of action and milestones, remediation plans, or information indicating the cyber threat, vulnerability, potential impacts or risk agencies or the state that could threaten the technology infrastructure critical to government operations and services, public safety or health is exempt from §29B-1-1 *et seq.* of this code.

NOTE: The purpose of this bill is to authorize the establishment of a cybersecurity framework for state agencies. The framework will be developed and administered by the Chief Information Security Officer within the Office of Technology. The bill creates a

minimum standard for cybersecurity controls for state agencies. The bill requires cybersecurity assessments to determine the status of state agencies with respect to cybersecurity. The bill provides exceptions from application and from disclosure of certain information.

The bill repeals §5A-6-4a.

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