WEST VIRGINIA LEGISLATURE

2021 REGULAR SESSION

Committee Substitute

for

House Bill 2763

BY DELEGATE LINVILLE

[Referred to the Committee on Technology and

Infrastructure then Government Organization;

reported March 9, 2021]

A BILL to amend the Code of West Virginia, 1931, as amended, by adding thereto a new article, designated §5A-6C-1, §5A-6C-2, §5A-6C-3, and §5A-6C-4, all relating to "West Virginia Cyber Incident Reporting;" providing for definitions; applying the scope to all state agencies within the executive branch, Constitutional officers, all local government entities, county boards of education, the judicial branch, and the legislative branch; providing criteria for reporting incidents; and providing for an annual report.

Be it enacted by the Legislature of West Virginia:

ARTICLE 6C. WEST VIRGINIA CYBER INCIDENT REPORTING.

§5A-6C-1. Definitions.

As used in this article:

"Cybersecurity Office" means the office created by §5A-6B-1 of this code.

"Incident" or "cybersecurity incident" means a violation, or imminent threat of violation, of computer security policies, acceptable use policies, or standard security practices.

§5A-6C-2. Scope.

This article shall apply to all state agencies within the executive branch, Constitutional Officers, all local government entities as defined by §7-1-1 or §8-1-2 of this code, county boards of education as defined by §18-1-1 of this code, the judicial branch and the legislative branch.

§5A-6C-3. Cyber Incident reporting; when required.

(a) Qualified cybersecurity incidents must be reported to the Cybersecurity Office before any citizen notification, but not later than 10 days following the agency's determination that a qualifying cybersecurity incident has occurred.

(b) A qualified cybersecurity incident meets one of the following criteria:

(1) State or federal law requires the reporting of the incident to regulatory or law-enforcement agencies or affected citizens;

(2) The entity's ability to conduct business is substantially affected; or

(3) The incident would be classified as Emergent, Severe, or High by the U.S. Cybersecurity and Infrastructure Security Agency.

(c) The report of the cybersecurity incident to the Cybersecurity Office shall contain at a minimum:

(1) The approximate date of the incident;

(2) The date incident was discovered;

(3) The nature of any data that may have been illegally obtained or accessed; and

(4) A list of the state and federal regulatory agencies, self-regulatory bodies, and foreign regulatory agencies to whom the notice has been or will be provided.

(d) The reporting method shall be provided by the Cybersecurity Office and made available to all agencies.

§5A-6C-4. Cybersecurity Office annual report.

(a) On or before December 31st each year, and when requested by the Legislature, the Cybersecurity Office shall provide a report to the Joint Committee on Government and Finance on the number and nature of incidents reported by Department during the preceding calendar year.

(b) The Cybersecurity Office shall also make recommendations, if any, on security standards or mitigation that should be adopted.

NOTE: The purpose of this bill is to provide a mechanism for reporting cyber incidents, and to provide for an annual report to the Joint Committee of the West Virginia Legislature.

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