WEST VIRGINIA CODE CHAPTER 5a ARTICLE 6C

§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 applies 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 Judiciary, and the Legislature.

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

(a) Qualified cybersecurity incidents shall be reported to the Cybersecurity Office before any citizen notification, but no later than 10 days following a determination that the entity experienced a qualifying cybersecurity incident.

(b) A qualified cybersecurity incident meets at least 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 ability of the entity that experienced the incident to conduct business is substantially affected; or

(3) The incident would be classified as emergency, 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 the 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 procedure for reporting cybersecurity incidents shall be established by the Cybersecurity Office and disseminated to the entities listed §5A-6C-2 of this code.

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

(a) On or before December 31 of each year, and when requested by the Legislature, the Cybersecurity Office shall provide a report to the Joint Committee on Government and Finance containing the number and nature of incidents reported to it during the preceding calendar year. The report shall be transmitted to the members of the committee electronically and shall be sent to the legislative librarian to be posted on the legislative website. No hard copy of the report shall be issued; however, a member shall be provided a hard copy upon request.

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