WEST VIRGINIA SECRETARY OF STATE

MAC WARNER

ADMINISTRATIVE LAW DIVISION

eFILED

7/30/2021 2:54:29 PM

Office of West Virginia
Secretary Of State

NOTICE OF AGENCY APPROVAL OF A PROPOSED RULE AND FILING WITH THE LEGISLATIVE RULE-MAKING REVIEW COMMITTEE

AGENCY: Office of Technology TITLE-SERIES: 163-03

RULE TYPE: Legislative Amendment to Existing Rule: No Repeal of existing rule: No

RULE NAME: 163-03 Cyber Reporting

PRIMARY CONTACT

NAME: Jennelle Jones

ADDRESS: Building 5 10th Floor
State Capitol Complex
Charleston, WV 25305

EMAIL: jennelle.h.jones@wv.gov

PHONE NUMBER: 304-352-4149

CITE STATUTORY AUTHORITY: 5A-6C-3 and 5A-6B-3

EXPLANATION OF THE STATUTORY AUTHORITY FOR THE LEGISLATIVE RULE, INCLUDING A DETAILED SUMMARY OF THE EFFECT OF EACH PROVISION OF THE LEGISLATIVE RULE WITH CITATION TO THE SPECIFIC STATUTORY PROVISION WHICH EMPOWERS THE AGENCY TO ENACT SUCH RULE PROVISION:

West Virginia Code 5A-6C-1 et seq., requires local and state government entities to report cyber incidents to the Cyber Security Office within the West Virginia Office of Technology. This rule provides the process to report the incidents.

IS THIS FILING SOLELY FOR THE SUNSET PROVISION REQUIREMENTS IN W. VA. CODE §29A-3-19(e)? No

IF YES, DO YOU CERTIFY THAT THE ONLY CHANGES TO THE RULE ARE THE FILING DATE, EFFECTIVE DATE AND AN EXTENSION OF THE SUNSET DATE? No

DATE eFiled FOR NOTICE OF HEARING OR PUBLIC COMMENT PERIOD: 6/15/2021

DATE OF PUBLIC HEARING(S) OR PUBLIC COMMENT PERIOD ENDED: 7/15/2021

COMMENTS RECEIVED: No

(IF YES, PLEASE UPLOAD IN THE COMMENTS RECEIVED FIELD COMMENTS RECEIVED AND RESPONSES TO COMMENTS)

PUBLIC HEARING: No

(IF YES, PLEASE UPLOAD IN THE PUBLIC HEARING FIELD PERSONS WHO APPEARED AT THE HEARING(S) AND TRANSCRIPTS)

RELEVANT FEDERAL STATUTES OR REGULATIONS: No

WHAT OTHER NOTICE, INCLUDING ADVERTISING, DID YOU GIVE OF THE HEARING?

None

SUMMARY OF THE CONTENT OF THE LEGISLATIVE RULE, AND A DETAILED DESCRIPTION OF THE RULE'S PURPOSE AND ALL PROPOSED CHANGES TO THE RULE:

The rule is a new rule and provides the reporting process for local and state government entities to report cyber incidents to the Cyber Security Office within the West Virginia Office of Technology.

STATEMENT OF CIRCUMSTANCES WHICH REQUIRE THE RULE:

During the 2021 Regular Session, House Bill 2763 was adopted, which requires state and local government entities to report cyber incidents to the Cyber Security Office within the West Virginia Office of Technology. This rule provides the process to report those incidents.

SUMMARIZE IN A CLEAR AND CONCISE MANNER THE OVERALL ECONOMIC IMPACT OF THE PROPOSED LEGISLATIVE RULE:

A. ECONOMIC IMPACT ON REVENUES OF STATE GOVERNMENT:

None

B. ECONOMIC IMPACT ON SPECIAL REVENUE ACCOUNTS:

None

C. ECONOMIC IMPACT OF THE LEGISLATIVE RULE ON THE STATE OR ITS RESIDENTS:

None

D. FISCAL NOTE DETAIL:

Effect of Proposal	Fiscal Year		
	2021 Increase/Decrease (use "-")	2022 Increase/Decrease (use "-")	Fiscal Year (Upon Full Implementation)
1. Estimated Total Cost	0	0	0
Personal Services	0	0	0
Current Expenses	0	0	
Repairs and Alterations			
Assets			
Other			
2. Estimated Total Revenues			

E. EXPLANATION OF ABOVE ESTIMATES (INCLUDING LONG-RANGE EFFECT):

N/A

BY CHOOSING 'YES', I ATTEST THAT THE PREVIOUS STATEMENT IS TRUE AND CORRECT.

Yes
Jennelle Jones -- By my signature, I certify that I am the person authorized to file legislative rules, in accordance with West Virginia Code §29A-3-11 and §39A-3-2.

TITLE 163
LEGISLATIVE RULE
WEST VIRGINIA OFFICE OF TECHNOLOGY

SERIES 3
CYBER REPORTING

§ 163-3-1. General Provisions.

1.1. Scope. -- This legislative rule establishes requirements relating to reporting of cyber incidents. This rule applies to all executive agencies, constitutional offices, local government entities, and county boards of education, as identified by W.Va. Code §5A-6C-2.

1.2. Authority. -- W. Va. Code §5A-6C-3 and §5A-6B-3.

1.3. Filing Date. --

1.4. Effective Date. --

1.5. Sunset Provision -- This rule shall terminate and have no further force or effect after August 1, 2027.

§163-3-2. Definitions.

2.1. "Cyber attack" means an attack via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure; or destroying the integrity of data or stealing controlled information.

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

2.3. "Cybersecurity Office" means the office created in W.Va. Code §5A-6B-1.

2.4. "Cyberspace" means a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, or embedded processors and controllers.

2.5. "Personally Identifiable Information" means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

2.6. "Protected Health Information" means individually identifiable health information that is transmitted by electronic media, maintained electronic media, or transmitted and maintained in any other form or medium. Protected health information does not include individually identifiable health information in education records covered by the Family Education Rights and Privacy Act, as amended, 20 U.S.C. 1232g; records described at 20 U.S.C. 1232g(a)(4)(B)(iv); or employment records held by a covered entity in its role as an employer.

§163-3-3. Reporting by any entity.

3.1. All entities shall report qualified cyber incidents to the Cybersecurity Office via online portal incident.wv.gov within 10 days of discovery of an incident. Notification to the Cybersecurity Office should be made before any citizen notification of the incident.

3.2. The report of a qualified cyber incident shall not include any personally identifiable information (PII), protected health information (PHI), passwords or login information.

§163-3-4. Reporting by executive branch agencies.

4.1. Any executive branch agency that discovers a cyber incident, cyber attack, substantial vulnerability or other electronic threat must immediately notify the Cybersecurity Office by submitting a report at incident.wv.gov if:

4.1.1. The incident, cyber attack, vulnerability, or threat has an immediate impact on state-owned or state-managed data, systems, or services; or

4.1.2. The incident, cyber attack, vulnerability, or threat can potentially impact state-owned or state-managed data, systems, or services.