WEST VIRGINIA LEGISLATURE

2023 REGULAR SESSION

ENROLLED

Senate Bill 734

By Senators Woodrum, Barrett, Hamilton, Hunt, Jeffries, Phillips, Queen, Smith, Stuart, Swope, and Weld

[Passed March 10, 2023; in effect 90 days from passage]

AN ACT to amend and reenact §5A-3-3c of the Code of West Virginia, 1931, as amended; to amend said code by adding thereto two new sections, designated §5A-6-4d and §5A-6-4e; and to amend and reenact §5A-6B-4 of said code, all relating to state data accessibility and infrastructure resiliency; requiring adoption of cloud computing services by state agencies; requiring development of a cloud strategy by Chief Information Officer; encouraging digitization of state agency forms; and requiring annual reporting on information technology modernization.

Be it enacted by the Legislature of West Virginia:

ARTICLE 3. PURCHASING DIVISION.

§5A-3-3c. Exemptions from purchasing requirements for contracts entered into as part of recovery from a declared state of emergency.

(a) The provisions of this article do not apply to contracts entered into during a state of emergency declared by the Governor pursuant to §15-5-6 of this code, so long as the contract is directly and solely related to the recovery from the declared state of emergency.

(b) The provisions of this article do not apply to the renewal of a contract entered into during a state of emergency declared pursuant to §15-5-6 of this code, if the contract is directly and solely related to the recovery from the declared state of emergency during which the contract was initially entered. For purposes of this subsection, recovery does not include permanent reconstruction after the initial state of emergency has ended.

(c) The provisions of this article do not apply to the purchase of goods or services from the federal government, or an agency thereof, if the purchase of those goods and services is directly and solely related to the recovery from a state of emergency declared pursuant to §15-5-6 of this code.

(d) At the discretion of the Chief Information Officer, the provisions of this article may not apply to the purchase, procurement, or implementation of information technology in response to a

qualified cyber security incident, as defined by §5A-6C-3 of this code: *Provided*, That the information technology is imminently necessary to protect the state's infrastructure or data.

(e) To qualify for the exemption contained in this section, the Director of the Division of Homeland Security and Emergency Management must certify that the contract or purchase is directly and solely related to the recovery from a declared state of emergency and attach a copy of the proclamation issued by the Governor's office to the certification. Such certifications shall be maintained by the Division of Homeland Security and Emergency Management until the contracts or purchase agreements have been fully executed.

(f) For purposes of this section, "directly and solely related" means that the goods or services being purchased or contracted for will be used for recovery from the state of emergency only and will not be used for any other purpose.

ARTICLE 6. OFFICE OF TECHNOLOGY.

§5A-6-4d. Responsibilities of the Chief Information Officer to implement information technology modernization.

(a) For the purposes of this section, "cloud computing service" means a service that enables on demand self-service network access to a shared pool of configurable computer resources including, but not limited to, data storage, analytics, electronic commerce, streaming services, mobile services, electronic mail, document sharing, and document editing which can be rapidly provided and released with minimal management effort or service provider interaction.

(b) The Chief Information Officer shall develop a comprehensive strategy and implement standards for the procurement, adoption, and utilization of cloud computing services by the state and its agencies. In developing the strategy, the Chief Information Officer may consult with other relevant state or federal agencies and relevant private sector stakeholders.

(c) When implementing the comprehensive strategy described in subsection (b) of this section, the Chief Information Officer may:

(1) Consider activities that accelerate the development of standards addressing

interoperability and portability of cloud computing services in collaboration with private sector stakeholders;

(2) Consider activities that advance the development of conformance testing to be performed by private sector stakeholders to support cloud computing standardization;

(3) Consider activities that support the development of appropriate security and architecture frameworks in consultation with private sector stakeholders; and

(4) Identify modern security control best practices to address security and privacy requirements, and to enable the use and adoption of cloud computing services, including practices defined in National Institute of Standards and Technology, Federal Risk and Authorization Management Program, and any equivalent state program adopted in West Virginia.

(d) Beginning on December 1, 2023, and on December 1 of each year after, the Chief Information Officer shall report annually the status of the state's comprehensive strategy described in subsection (b) of this section to the Joint Committee on Government and Finance and to the Governor. To assist in the creation of the report, all relevant state agencies shall cooperate with the Chief Information Officer and provide any information required by the Chief Information Officer in an accurate and timely manner.

§5A-6-4e. Digitization of state forms.

(a)(1) All state agencies shall explore existing paper-based forms and applications so that said forms and applications can be made conveniently available to state residents.

(2) The Chief Information Officer may work collaboratively with private sector vendors to establish contracts and services to enable state agencies in modernizing government services to be delivered through a digital media.

(3) The Chief Information Officer shall work with all state agencies to ensure that all paper-based forms and applications are made available to state residents through digital media by no later than July 1, 2025.

ARTICLE 6B. CYBER SECURITY PROGRAM.

§5A-6B-4. Responsibilities of agencies for cybersecurity.

State agencies and other entities 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 analysis and evaluation of each agency or entity's cybersecurity readiness, ability to keep user data safe, data classifications, and other steps that the agency or entity has taken towards information technology modernization that are consistent with the objectives of §5A-6-4d and §5A-6-4e 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 summary of each state agency's report submitted

pursuant to §5A-6B-4 of this code regarding the agency's cybersecurity readiness and the agency's information technology modernization efforts.