Senate File 2391

S-5079

Amend Senate File 2391 as follows:

1. Page 1, by striking lines 4 through 6 and inserting <subdivision of the state, in consultation with the department of public safety and the department of homeland security and emergency management, to expend revenue received from taxpayers for payment to a person responsible for, or reasonably believed to be responsible for, a ransomware attack pursuant to section 8H.3.>

2. Page 1, after line 9 by inserting:

<___. *"Critical infrastructure"* means the same as defined in section 29C.24.>

3. By striking page 1, line 25, through page 2, line 6, and inserting:

<Sec. ___. NEW SECTION. **8H.2 Requirement to report a ransomware attack.** If the state or a political subdivision of the state is subject to a ransomware attack, the state or the political subdivision shall provide notice of the ransomware attack to the office of the chief information officer following discovery of the ransomware attack. The notice shall be provided in the most expeditious manner possible and without unreasonable delay. The office of the chief information officer shall adopt rules establishing notification procedures pursuant to this section.

Sec. ___. NEW SECTION. **8H.3 Revenue received from taxpayers — prohibition — ransomware.**

1. Except as provided in subsection 2 or 3, the state or a political subdivision of the state shall not expend revenue received from taxpayers for payment to a person responsible for, or reasonably believed to be responsible for, a ransomware attack.

2. The office of the chief information officer, in consultation with the department of public safety and the department of homeland security and emergency management, may authorize the state or a political subdivision of the state to expend revenue otherwise prohibited pursuant to subsection 1 in

the event of any of the following:

a. A critical or emergency situation as defined by the department of homeland security and emergency management.

b. A ransomware attack affecting critical infrastructure within the state or a political subdivision of the state.

3. The state or a political subdivision of the state may expend revenue otherwise prohibited pursuant to subsection 1 in the event of a ransomware attack affecting an officer or employee of the judicial branch.

Sec. ___. NEW SECTION. **8H.4 Payments for insurance.**

The state or a political subdivision of the state may use revenue received from taxpayers to pay premiums, deductibles, and other costs associated with an insurance policy related to cybersecurity or ransomware attacks only if the state or the political subdivision first exhausts all other reasonable means of mitigating a potential ransomware attack. Subject to section 8H.3, subsections 2 and 3, nothing in this section shall be construed to authorize the state or a political subdivision of the state to make a direct payment using revenue received from taxpayers to a person responsible for, or reasonably believed to be responsible for, a ransomware attack.

Sec. ___. NEW SECTION. **8H.5 Confidential records.**

Information related to all of the following shall be considered a confidential record under section 22.7:

1. Insurance coverage maintained by the state or a political subdivision of the state related to cybersecurity or a ransomware attack.

2. Payment by the state or a political subdivision of the state to a person responsible for, or believed to be responsible for, a ransomware attack pursuant to section 8H.3.>

4. Page 2, after line 9 by inserting:

<Sec. ___. RULEMAKING. The office of the chief information officer shall prepare a notice of intended action for the adoption of rules to administer this Act. The notice of intended action shall be submitted to the administrative

rules coordinator and the administrative code editor as soon as practicable, but no later than October 1, 2020. However, nothing in this section authorizes the office of the chief information officer to adopt rules under section 17A.4, subsection 3, or section 17A.5, subsection 2, paragraph "b".

Sec. ___. EFFECTIVE DATE.

1. Except as provided in subsection 2, this Act takes effect July 1, 2021.

2. The section of this Act requiring the office of the chief information officer to prepare a notice of intended action for the adoption of rules to administer this Act takes effect upon enactment.>

5. Title page, by striking lines 1 through 3 and inserting <An Act prohibiting the state or a political subdivision of the state from expending revenue received from taxpayers for payment to persons responsible for ransomware attacks, and including effective date provisions.>

6. By renumbering, redesignating, and correcting internal references as necessary.

_____

ZACH NUNN