HOUSE FILE 554
BY COMMITTEE ON ECONOMIC
GROWTH AND TECHNOLOGY

(SUCCESSOR TO HSB 153)

A BILL FOR

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.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:

Section 1. Section 8B.4, Code 2023, is amended by adding the following new subsection:

NEW SUBSECTION. 18A. Authorize the state or a political subdivision of the state, not including a municipal utility, 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.

Sec. 2. NEW SECTION. **8H.1 Definitions.**

As used in this chapter, unless the context otherwise requires:

1. *"Critical infrastructure"* means the same as defined in section 29C.24. *"Critical infrastructure"* includes real and personal property and equipment owned or used to provide fire fighting, law enforcement, medical, or other emergency services.

2. *"Encryption"* means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.

3. *"Political subdivision"* means a city, county, township, or school district. *"Political subdivision"* does not include a municipal utility.

4. *"Ransomware attack"* means carrying out until payment is made, or threatening to carry out until payment is made, any of the following actions:

a. An act declared unlawful pursuant to section 715.4.

b. A breach of security as defined in section 715C.1.

c. The use of any form of software that results in the unauthorized encryption of data, the denial of access to data, the denial of access to a computer, or the denial of access to a computer system.

Sec. 3. 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. 4. 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 tax 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 shall notify the department of public safety and the department of homeland security and emergency management, and may authorize the state or a political subdivision of the state to expend tax 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, or when the department of homeland security and emergency management determines the expenditure of tax revenue is in the public interest.

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 tax revenue otherwise prohibited pursuant to subsection 1 in the event of a ransomware attack affecting an officer or employee of the judicial branch.

Sec. 5. 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 at any time 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. 6. 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.

Sec. 7. LEGISLATIVE INTENT. It is the intent of the general assembly that the state and the political subdivisions of the state have tested cybersecurity mitigation plans and policies.

Sec. 8. 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, 2023. 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. 9. EFFECTIVE DATE.

1. Except as provided in subsection 2, this Act takes effect July 1, 2024.

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, being deemed of immediate importance, takes effect upon enactment.

EXPLANATION

The inclusion of this explanation does not constitute agreement with the explanation's substance by the members of the general assembly.

This bill prohibits the state or a political subdivision of the state from expending revenue received from taxpayers for payment to persons responsible for ransomware attacks.

The bill defines "critical infrastructure" to mean real and personal property and equipment owned or used by communication and video networks, gas distribution systems, water and wastewater pipeline systems, and electric generation, transmission, and distribution systems, including related support facilities, which network or system provides service to more than one customer or person as defined in Code section 29C.24. "Critical infrastructure" includes but is not limited to buildings, structures, offices, lines, poles, pipes, and equipment, as well as real and personal property owned or used to provide fire fighting, law enforcement, medical, or other emergency services. The bill defines "encryption" as the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key. The bill defines "political subdivision" as a city, county, township, or school district. The bill defines "ransomware attack" to mean carrying out until payment is made, or threatening to carry out until payment is made, including an act declared unlawful pursuant to Code section 715.4, a "breach of security" as defined in Code section 715C.1, or the use of any form of software that results in the unauthorized encryption of data, the denial of access to data, the denial of access to a computer, or the denial of access to a computer system.

The bill requires that when the state or a political

subdivision of the state is subject to a ransomware attack and discovers the attack, the state or political subdivision shall expeditiously provide notice to the office of the chief information officer. The office of the chief information officer shall adopt rules establishing notification procedures.

The bill provides that 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.

The bill allows the office of the chief information officer to authorize such expenditures in the event of a critical or emergency situation as determined by the department of homeland security and emergency management and requires the office of the chief information officer to notify the departments of the expenditures. The bill provides that information related to a political subdivision's insurance coverage for cybersecurity or ransomware attack shall be considered confidential records.

The bill provides that the state or a political subdivision of the state may use taxpayer revenue to pay for cybersecurity insurance or related ransomware insurance at any time if the state or political subdivision first exhausts all other reasonable means of mitigating a potential ransomware attack.

The bill includes a legislative intent section, which provides that it is the intent of the general assembly that the state and political subdivisions of the state have tested cybersecurity mitigation plans and policies.

The bill takes effect July 1, 2024, except for the section of the bill requiring the office of the chief information officer to prepare a notice of intended action (NOIA) for the adoption of rules, which takes effect upon enactment. The NOIA must be submitted to the administrative rules coordinator and administrative code editor as soon as possible and no later than October 1, 2023. The bill does not authorize the office of the chief information officer to adopt emergency rules under Code section 17A.4(3) or Code section 17A.5(2)(b).