Senate File 2391 - Introduced

SENATE FILE 2391
BY COMMITTEE ON STATE GOVERNMENT

(SUCCESSOR TO SF 2080)

A BILL FOR

An Act prohibiting the state and political subdivisions of the state from expending public moneys for payment to persons responsible for ransomware attacks.

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

Section 1. Section 8B.4, Code 2020, is amended by adding the following new subsection:

NEW SUBSECTION. 17A. Authorize the state or a political subdivision of the state to expend public moneys for payment to a person responsible for, or reasonably believed to be responsible for, a ransomware attack pursuant to section 8H.2.

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

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

1. *"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.

2. *"Political subdivision"* means a city, county, township, or school district.

3. *"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 Public moneys — prohibition — ransomware — confidential records.**

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

2. Notwithstanding subsection 1, the office of the chief information officer may authorize the state or a political subdivision of the state to expend public moneys for payment to a person responsible for, or reasonably believed to be responsible for, a ransomware attack in the event of a critical

or emergency situation as determined by the department of homeland security and emergency management created in section 29C.5.

3. Information related to a political subdivision's insurance coverage for cybersecurity or a ransomware attack shall be considered confidential records under section 22.7.

Sec. 4. 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.

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 and a political subdivision of the state from expending public moneys for payment to persons responsible for ransomware attacks.

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, any of the following: 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 provides that the state and a political subdivision of the state shall not expend public moneys 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. The bill provides that information related to a political subdivision's insurance coverage for cybersecurity or ransomware attack shall be considered confidential records under Code section 22.7.

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.