

House Study Bill 691 - Introduced

HOUSE FILE _____
BY (PROPOSED COMMITTEE ON
INFORMATION TECHNOLOGY BILL
BY CHAIRPERSON LOHSE)

A BILL FOR

1 An Act prohibiting the state or a political subdivision of the
2 state from expending revenue received from taxpayers for
3 payment to persons responsible for ransomware attacks, and
4 including effective date provisions.
5 BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:

1 Section 1. Section 8B.4, Code 2022, is amended by adding the
2 following new subsection:

3 NEW SUBSECTION. 18A. Authorize the state or a political
4 subdivision of the state, not including a municipal utility,
5 in consultation with the department of public safety and the
6 department of homeland security and emergency management, to
7 expend revenue received from taxpayers for payment to a person
8 responsible for, or reasonably believed to be responsible for,
9 a ransomware attack pursuant to section 8H.3.

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

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

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

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

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

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

28 a. An act declared unlawful pursuant to section 715.4.

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

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

34 Sec. 3. NEW SECTION. 8H.2 **Requirement to report a**
35 **ransomware attack.**

1 If the state or a political subdivision of the state is
2 subject to a ransomware attack, the state or the political
3 subdivision shall provide notice of the ransomware attack to
4 the office of the chief information officer following discovery
5 of the ransomware attack. The notice shall be provided in
6 the most expeditious manner possible and without unreasonable
7 delay. The office of the chief information officer shall adopt
8 rules establishing notification procedures pursuant to this
9 section.

10 Sec. 4. NEW SECTION. **8H.3 Revenue received from taxpayers**
11 **— prohibition — ransomware.**

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

17 2. The office of the chief information officer, in
18 consultation with the department of public safety and the
19 department of homeland security and emergency management, may
20 authorize the state or a political subdivision of the state to
21 expend tax revenue otherwise prohibited pursuant to subsection
22 1 in the event of any of the following:

23 a. A critical or emergency situation as defined by the
24 department of homeland security and emergency management,
25 or when the department of homeland security and emergency
26 management determines the expenditure of tax revenue is in the
27 public interest.

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

30 3. The state or a political subdivision of the state may
31 expend tax revenue otherwise prohibited pursuant to subsection
32 1 in the event of a ransomware attack affecting an officer or
33 employee of the judicial branch.

34 Sec. 5. NEW SECTION. **8H.4 Payments for insurance.**

35 The state or a political subdivision of the state may use

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

11 **Sec. 6. NEW SECTION. 8H.5 Confidential records.**

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

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

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

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

23 **Sec. 8. RULEMAKING.** The office of the chief information
24 officer shall prepare a notice of intended action for the
25 adoption of rules to administer this Act. The notice of
26 intended action shall be submitted to the administrative
27 rules coordinator and the administrative code editor as soon
28 as practicable, but no later than October 1, 2022. However,
29 nothing in this section authorizes the office of the chief
30 information officer to adopt rules under section 17A.4,
31 subsection 3, or section 17A.5, subsection 2, paragraph "b".

32 **Sec. 9. EFFECTIVE DATE.**

33 1. Except as provided in subsection 2, this Act takes effect
34 July 1, 2023.

35 2. The section of this Act requiring the office of the chief

1 information officer to prepare a notice of intended action for
2 the adoption of rules to administer this Act, being deemed of
3 immediate importance, takes effect upon enactment.

4

EXPLANATION

5

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

6

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

10 The bill defines "critical infrastructure" to mean
11 real and personal property and equipment owned or used by
12 communication and video networks, gas distribution systems,
13 water and wastewater pipeline systems, and electric generation,
14 transmission, and distribution systems, including related
15 support facilities, which network or system provides service
16 to more than one customer or person as defined in Code section
17 29C.24. "Critical infrastructure" includes but is not limited
18 to buildings, structures, offices, lines, poles, pipes, and
19 equipment, as well as real and personal property owned or
20 used to provide fire fighting, law enforcement, medical, or
21 other emergency services. The bill defines "encryption" as
22 the use of an algorithmic process to transform data into a
23 form in which the data is rendered unreadable or unusable
24 without the use of a confidential process or key. The bill
25 defines "political subdivision" as a city, county, township,
26 or school district. The bill defines "ransomware attack" to
27 mean carrying out until payment is made, or threatening to
28 carry out until payment is made, including an act declared
29 unlawful pursuant to Code section 715.4, a "breach of security"
30 as defined in Code section 715C.1, or the use of any form
31 of software that results in the unauthorized encryption of
32 data, the denial of access to data, the denial of access to a
33 computer, or the denial of access to a computer system.
34 The bill requires that when the state or a political
35 subdivision of the state is subject to a ransomware attack

1 and discovers the attack, the state or political subdivision
2 shall expeditiously provide notice to the office of the chief
3 information officer. The office of the chief information
4 officer shall adopt rules establishing notification procedures.

5 The bill provides that the state or a political subdivision
6 of the state shall not expend revenue received from taxpayers
7 for payment to a person responsible for, or reasonably believed
8 to be responsible for, a ransomware attack.

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

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

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

25 The bill takes effect July 1, 2023, except for the section
26 of the bill requiring the office of the chief information
27 officer to prepare a notice of intended action (NOIA) for the
28 adoption of rules, which takes effect upon enactment. The NOIA
29 must be submitted to the administrative rules coordinator and
30 administrative code editor as soon as possible and no later
31 than October 1, 2022. The bill does not authorize the office
32 of the chief information officer to adopt emergency rules under
33 Code section 17A.4(3) or Code section 17A.5(2)(b).