

**Senate File 2391 - Introduced**

SENATE FILE 2391  
BY COMMITTEE ON STATE  
GOVERNMENT

(SUCCESSOR TO SF 2080)

**A BILL FOR**

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

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

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

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

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

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

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

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

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

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

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

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

25 Sec. 3. NEW SECTION. 8H.2 **Public moneys — prohibition —**  
26 **ransomware — confidential records.**

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

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

1 or emergency situation as determined by the department of  
2 homeland security and emergency management created in section  
3 29C.5.

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

7 Sec. 4. LEGISLATIVE INTENT. It is the intent of the general  
8 assembly that the state and the political subdivisions of the  
9 state have tested cybersecurity mitigation plans and policies.

10

EXPLANATION

11

The inclusion of this explanation does not constitute agreement with

12

the explanation's substance by the members of the general assembly.

13

This bill prohibits the state and a political subdivision of  
14 the state from expending public moneys for payment to persons  
15 responsible for ransomware attacks.

16

The bill defines "encryption" as the use of an algorithmic  
17 process to transform data into a form in which the data  
18 is rendered unreadable or unusable without the use of a  
19 confidential process or key. The bill defines "political  
20 subdivision" as a city, county, township, or school district.  
21 The bill defines "ransomware attack" to mean carrying out until  
22 payment is made, or threatening to carry out until payment is  
23 made, any of the following: an act declared unlawful pursuant  
24 to Code section 715.4; a "breach of security" as defined in  
25 Code section 715C.1; or the use of any form of software that  
26 results in the unauthorized encryption of data, the denial of  
27 access to data, the denial of access to a computer, or the  
28 denial of access to a computer system.

29

The bill provides that the state and a political subdivision  
30 of the state shall not expend public moneys for payment  
31 to a person responsible for, or reasonably believed to be  
32 responsible for, a ransomware attack.

33

The bill allows the office of the chief information officer  
34 to authorize such expenditures in the event of a critical or  
35 emergency situation as determined by the department of homeland

1 security and emergency management. The bill provides that  
2 information related to a political subdivision's insurance  
3 coverage for cybersecurity or ransomware attack shall be  
4 considered confidential records under Code section 22.7.

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