

**House Study Bill 555 - Introduced**

HOUSE FILE \_\_\_\_\_

BY (PROPOSED COMMITTEE ON  
INFORMATION TECHNOLOGY BILL  
BY CHAIRPERSON LOHSE)

**A BILL FOR**

1 An Act relating to affirmative defenses for entities using  
2 cybersecurity programs and electronic transactions recorded  
3 by blockchain technology.

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

1 Section 1. Section 554D.103, subsections 8, 9, and 17, Code  
2 2022, are amended to read as follows:

3 8. "*Electronic record*" means a record created, generated,  
4 sent, communicated, received, or stored by electronic means.  
5 "*Electronic record*" includes any record or contract secured  
6 through distributed ledger technology or blockchain technology.

7 9. "*Electronic signature*" means an electronic sound, symbol,  
8 or process attached to or logically associated with a record  
9 and executed or adopted by a person with the intent to sign  
10 the record. "*Electronic signature*" includes a signature that  
11 is secured through distributed ledger technology or blockchain  
12 technology.

13 17. "*State*" means a state of the United States, the District  
14 of Columbia, Puerto Rico, the United States Virgin Islands, or  
15 any territory or insular possession subject to the jurisdiction  
16 of the United States. "*State*" includes an Indian tribe or  
17 band, or Alaskan ~~native~~ Native village, which is recognized by  
18 federal law or formally acknowledged by a state.

19 Sec. 2. NEW SECTION. 554E.1 Definitions.

20 As used in this chapter:

21 1. "*Business*" means any limited liability company, limited  
22 liability partnership, corporation, sole proprietorship,  
23 association, or other group, however organized and whether  
24 operating for profit or not for profit, including a financial  
25 institution organized, chartered, or holding a license  
26 authorizing operation under the laws of this state, any other  
27 state, the United States, or any other country, or the parent  
28 or subsidiary of any of the foregoing.

29 2. "*Covered entity*" means a business that accesses,  
30 maintains, communicates, or processes personal information  
31 or restricted information in or through one or more systems,  
32 networks, or services located in or outside this state.

33 3. "*Data breach*" means unauthorized access to and  
34 acquisition of computerized data that compromises the security  
35 or confidentiality of personal information or restricted

1 information owned by or licensed to a covered entity and that  
2 causes, reasonably is believed to have caused, or reasonably is  
3 believed will cause a material risk of identity theft or other  
4 fraud to person or property. "Data breach" does not include any  
5 of the following:

6 a. Good-faith acquisition of personal information or  
7 restricted information by the covered entity's employee or  
8 agent for the purposes of the covered entity, provided that  
9 the personal information or restricted information is not used  
10 for an unlawful purpose or subject to further unauthorized  
11 disclosure.

12 b. Acquisition of personal information or restricted  
13 information pursuant to a search warrant, subpoena, or other  
14 court order, or pursuant to a subpoena, order, or duty of a  
15 regulatory state agency.

16 4. "Encrypted" means the use of an algorithmic process to  
17 transform data into a form in which there is a low probability  
18 of assigning meaning without use of a confidential process or  
19 key.

20 5. "Individual" means a natural person.

21 6. "Personal information" means an individual's name,  
22 consisting of the individual's first name or first initial and  
23 last name, in combination with and linked to any one or more  
24 of the following data elements, when the data elements are not  
25 encrypted, redacted, or altered by any method or technology in  
26 such a manner that the data elements are unreadable:

27 a. Social security number.

28 b. Driver's license number or state identification card  
29 number.

30 c. Account number or credit or debit card number, in  
31 combination with and linked to any required security code,  
32 access code, or password that would permit access to an  
33 individual's financial account.

34 d. "Personal information" does not include publicly  
35 available information that is lawfully made available to the

1 general public from federal, state, or local government records  
2 or any of the following media that are widely distributed:

3 (1) Any news, editorial, or advertising statement published  
4 in any bona fide newspaper, journal, or magazine, or broadcast  
5 over radio or television.

6 (2) Any gathering or furnishing of information or news by  
7 any bona fide reporter, correspondent, or news bureau to news  
8 media identified in this paragraph.

9 (3) Any publication designed for and distributed to members  
10 of any bona fide association or charitable or fraternal  
11 nonprofit corporation.

12 (4) Any type of media similar in nature to any item, entity,  
13 or activity identified in this paragraph.

14 7. "Redacted" means altered or truncated so that no more  
15 than the last four digits of a social security number, driver's  
16 license number, state identification card number, account  
17 number, or credit or debit card number is accessible as part  
18 of the data.

19 8. "Restricted information" means any information about  
20 an individual, other than personal information, that,  
21 alone or in combination with other information, including  
22 personal information, can be used to distinguish or trace the  
23 individual's identity or that is linked or linkable to an  
24 individual, if the information is not encrypted, redacted, or  
25 altered by any method or technology in such a manner that the  
26 information is unreadable, and the breach of which is likely  
27 to result in a material risk of identity theft or other fraud  
28 to person or property.

29 Sec. 3. NEW SECTION. 554E.2 Affirmative defenses.

30 1. A covered entity seeking an affirmative defense under  
31 this chapter shall do one of the following:

32 a. Create, maintain, and comply with a written cybersecurity  
33 program that contains administrative, technical, and physical  
34 safeguards for the protection of personal information and that  
35 reasonably conforms to an industry-recognized cybersecurity

1 framework, as described in section 554E.3.

2 *b.* Create, maintain, and comply with a written cybersecurity  
3 program that contains administrative, technical, and physical  
4 safeguards for the protection of both personal information  
5 and restricted information and that reasonably conforms to an  
6 industry-recognized cybersecurity framework, as described in  
7 section 554E.3.

8 2. A covered entity's cybersecurity program shall be  
9 designed to do all of the following with respect to the  
10 information described in subsection 1, paragraph "a" or "b", as  
11 applicable:

12 *a.* Protect the security and confidentiality of the  
13 information.

14 *b.* Protect against any anticipated threats or hazards to the  
15 security or integrity of the information.

16 *c.* Protect against unauthorized access to and acquisition  
17 of the information that is likely to result in a material risk  
18 of identity theft or other fraud to the individual to whom the  
19 information relates.

20 3. The scale and scope of a covered entity's cybersecurity  
21 program under subsection 1, paragraph "a" or "b", as applicable,  
22 is appropriate if the cybersecurity program is based on all of  
23 the following factors:

24 *a.* The size and complexity of the covered entity.

25 *b.* The nature and scope of the activities of the covered  
26 entity.

27 *c.* The sensitivity of the information to be protected.

28 *d.* The cost and availability of tools to improve information  
29 security and reduce vulnerabilities.

30 *e.* The resources available to the covered entity.

31 4. *a.* A covered entity that satisfies subsection 1,  
32 paragraph "a", and subsections 2 and 3, is entitled to an  
33 affirmative defense to any cause of action sounding in tort  
34 that is brought under the laws of this state or in the courts  
35 of this state and that alleges that the failure to implement

1 reasonable information security controls resulted in a data  
2 breach concerning personal information.

3     *b.* A covered entity that satisfies subsection 1, paragraph  
4 “*b*”, and subsections 2 and 3, is entitled to an affirmative  
5 defense to any cause of action sounding in tort that is brought  
6 under the laws of this state or in the courts of this state  
7 and that alleges that the failure to implement reasonable  
8 information security controls resulted in a data breach  
9 concerning personal information or restricted information.

10     Sec. 4. NEW SECTION.   **554E.3 Cybersecurity program**  
11 **framework.**

12     1. A covered entity’s cybersecurity program, as  
13 described in section 554E.2, reasonably conforms to an  
14 industry-recognized cybersecurity framework for purposes of  
15 section 554E.2 if any of the following are true:

16     *a.* (1) The cybersecurity program reasonably conforms to the  
17 current version of any of the following or any combination of  
18 the following, subject to subparagraph (2) and subsection 2:

19         (i) The framework for improving critical infrastructure  
20 cybersecurity developed by the national institute of standards  
21 and technology.

22         (ii) National institute of standards and technology special  
23 publication 800-171.

24         (iii) National institute of standards and technology special  
25 publications 800-53 and 800-53a.

26         (iv) The federal risk and authorization management program  
27 security assessment framework.

28         (v) The center for internet security critical security  
29 controls for effective cyber defense.

30         (vi) The international organization for  
31 standardization/international electrotechnical commission 27000  
32 family — information security management systems.

33     (2) When a final revision to a framework listed in  
34 subparagraph (1) is published, a covered entity whose  
35 cybersecurity program reasonably conforms to that framework

1 shall reasonably conform to the revised framework not later  
2 than one year after the publication date stated in the  
3 revision.

4 *b.* (1) The covered entity is regulated by the state, by  
5 the federal government, or both, or is otherwise subject to  
6 the requirements of any of the laws or regulations listed  
7 below, and the cybersecurity program reasonably conforms to  
8 the entirety of the current version of any of the following,  
9 subject to subparagraph (2):

10 (a) The security requirements of the federal Health  
11 Insurance Portability and Accountability Act of 1996, as set  
12 forth in 45 C.F.R. pt. 164, subpt. C.

13 (b) Title V of the federal Gramm-Leach-Bliley Act of 1999,  
14 Pub. L. No. 106-102, as amended.

15 (c) The federal Information Security Modernization Act of  
16 2014, Pub. L. No. 113-283.

17 (d) The federal Health Information Technology for Economic  
18 and Clinical Health Act as set forth in 45 C.F.R. pt. 162.

19 (2) When a framework listed in subparagraph (1) is amended,  
20 a covered entity whose cybersecurity program reasonably  
21 conforms to that framework shall reasonably conform to the  
22 amended framework not later than one year after the effective  
23 date of the amended framework.

24 *c.* (1) The cybersecurity program reasonably complies  
25 with both the current version of the payment card industry  
26 data security standard and conforms to the current version of  
27 another applicable industry-recognized cybersecurity framework  
28 listed in paragraph "a", subject to subparagraph (2) and  
29 subsection 2.

30 (2) When a final revision to the payment card industry  
31 data security standard is published, a covered entity whose  
32 cybersecurity program reasonably complies with that standard  
33 shall reasonably comply with the revised standard not later  
34 than one year after the publication date stated in the  
35 revision.

1 2. If a covered entity's cybersecurity program reasonably  
2 conforms to a combination of industry-recognized cybersecurity  
3 frameworks, or complies with a standard, as in the case of the  
4 payment card industry data security standard, as described in  
5 subsection 1, paragraph "a" or "c", and two or more of those  
6 frameworks are revised, the covered entity whose cybersecurity  
7 program reasonably conforms to or complies with, as applicable,  
8 those frameworks shall reasonably conform to or comply with, as  
9 applicable, all of the revised frameworks not later than one  
10 year after the latest publication date stated in the revisions.

11 **Sec. 5. NEW SECTION. 554E.4 Causes of actions.**

12 This chapter shall not be construed to provide a private  
13 right of action, including a class action, with respect to any  
14 act or practice regulated under those sections.

15 **EXPLANATION**

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

18 This bill relates to cybersecurity programs and blockchain  
19 technology. The bill changes the definitions of "electronic  
20 record" and "electronic signature" in the uniform electronic  
21 transactions Act to include blockchain technology.

22 The bill creates affirmative defenses for entities using  
23 cybersecurity programs and provides definitions. The  
24 bill provides that a covered entity seeking an affirmative  
25 defense must use a cybersecurity program for the protection  
26 of personal information or both personal information and  
27 restricted information and the cybersecurity program must  
28 reasonably conform to an industry-recognized cybersecurity  
29 framework. A cybersecurity program must protect the security  
30 and confidentiality of the information, protect against any  
31 anticipated threats to the information, and protect against  
32 unauthorized access to and acquisition of the information that  
33 is likely to result in a material risk of identity theft. A  
34 cybersecurity program scale and scope should be based upon  
35 the size and complexity of the covered entity, the nature



1 and scope of the covered entity's activities, sensitivity  
2 of the information, and the cost and availability of tools  
3 and resources to improve information security. A covered  
4 entity that satisfies the above requirements is entitled to  
5 an affirmative defense to a tort claim that alleges that the  
6 failure to implement reasonable information security controls  
7 resulted in a data breach concerning personal information or  
8 restricted information.

9       The bill provides industry-recognized cybersecurity  
10 frameworks that the covered entity should follow and reasonably  
11 comply to in order to qualify for the affirmative defense.

12       The bill does not provide a private right to action,  
13 including a class action.