

House File 553 - Reprinted

HOUSE FILE 553
BY COMMITTEE ON ECONOMIC
GROWTH AND TECHNOLOGY

(SUCCESSOR TO HSB 154)

(As Amended and Passed by the House March 15, 2023)

A BILL FOR

- 1 An Act relating to affirmative defenses for entities using
- 2 cybersecurity programs.
- 3 BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF IOWA:

1 Section 1. NEW SECTION. 554G.1 Definitions.

2 As used in this chapter:

3 1. "*Business*" means any limited liability company, limited
4 liability partnership, corporation, sole proprietorship,
5 association, or other group, however organized and whether
6 operating for profit or not for profit, including a financial
7 institution organized, chartered, or holding a license
8 authorizing operation under the laws of this state, any other
9 state, the United States, or any other country, or the parent
10 or subsidiary of any of the foregoing, including an entity
11 organized under chapter 28E. "*Business*" does not include a
12 municipality as defined in section 670.1.

13 2. "*Contract*" means the same as defined in section 554D.103.

14 3. "*Covered entity*" means a business that accesses,
15 receives, stores, maintains, communicates, or processes
16 personal information or restricted information in or through
17 one or more systems, networks, or services located in or
18 outside this state.

19 4. "*Data breach*" means an intentional or unintentional
20 action that could result in electronic records owned, licensed
21 to, or otherwise protected by a covered entity being viewed,
22 copied, modified, transmitted, or destroyed in a manner that
23 is reasonably believed to have or may cause material risk of
24 identity theft, fraud, or other injury or damage to person or
25 property. "*Data breach*" does not include any of the following:

26 a. Good-faith acquisition of personal information or
27 restricted information by the covered entity's employee or
28 agent for the purposes of the covered entity, provided that
29 the personal information or restricted information is not used
30 for an unlawful purpose or subject to further unauthorized
31 disclosure.

32 b. Acquisition or disclosure of personal information or
33 restricted information pursuant to a search warrant, subpoena,
34 or other court order, or pursuant to a subpoena, order, or duty
35 of a regulatory state agency.

1 5. "*Distributed ledger technology*" means the same as defined
2 in section 554E.1.

3 6. "*Electronic record*" means the same as defined in section
4 554D.103.

5 7. "*Encrypted*" means the use of an algorithmic process to
6 transform data into a form for which there is a low probability
7 of assigning meaning without use of a confidential process or
8 key.

9 8. "*Individual*" means a natural person.

10 9. "*Maximum probable loss*" means the greatest damage
11 expectation that could reasonably occur from a data breach.
12 For purposes of this subsection, "*damage expectation*" means the
13 total value of possible damage multiplied by the probability
14 that damage would occur.

15 10. a. "*Personal information*" means any information
16 relating to an individual who can be identified, directly or
17 indirectly, in particular by reference to an identifier such
18 as a name, an identification number, social security number,
19 driver's license number or state identification card number,
20 passport number, account number or credit or debit card number,
21 location data, biometric data, an online identifier, or to
22 one or more factors specific to the physical, physiological,
23 genetic, mental, economic, cultural, or social identity of that
24 individual.

25 b. "*Personal information*" does not include publicly
26 available information that is lawfully made available to the
27 general public from federal, state, or local government records
28 or any of the following media that are widely distributed:

29 (1) Any news, editorial, or advertising statement published
30 in any bona fide newspaper, journal, or magazine, or broadcast
31 over radio, television, or the internet.

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

35 (3) Any publication designed for and distributed to members

1 of any bona fide association or charitable or fraternal
2 nonprofit business.

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

5 11. "*Record*" means the same as defined in section 554D.103.

6 12. "*Redacted*" means altered, truncated, or anonymized so
7 that, when applied to personal information, the data can no
8 longer be attributed to a specific individual without the use
9 of additional information.

10 13. "*Restricted information*" means any information about
11 an individual, other than personal information, or business
12 that, alone or in combination with other information, including
13 personal information, can be used to distinguish or trace the
14 identity of the individual or business, or that is linked or
15 linkable to an individual or business, if the information is
16 not encrypted, redacted, tokenized, or altered by any method or
17 technology in such a manner that the information is anonymized,
18 and the breach of which is likely to result in a material risk
19 of identity theft or other fraud to person or property.

20 14. "*Smart contract*" means the same as defined in section
21 554E.1.

22 15. "*Transaction*" means a sale, trade, exchange, transfer,
23 payment, or conversion of virtual currency or other digital
24 asset or any other property or any other action or set of
25 actions occurring between two or more persons relating to the
26 conduct of business, commercial, or governmental affairs.

27 Sec. 2. NEW SECTION. 554G.2 Affirmative defenses.

28 1. A covered entity seeking an affirmative defense under
29 this chapter shall create, maintain, and comply with a written
30 cybersecurity program that contains administrative, technical,
31 operational, and physical safeguards for the protection of both
32 personal information and restricted information.

33 2. A covered entity's cybersecurity program shall be
34 designed to do all of the following:

35 a. Continually evaluate and mitigate any reasonably

1 anticipated internal or external threats or hazards that could
2 lead to a data breach.

3 b. Periodically evaluate no less than annually the maximum
4 probable loss attainable from a data breach.

5 c. Communicate to any affected parties the extent of any
6 risk posed and any actions the affected parties could take to
7 reduce any damages if a data breach is known to have occurred.

8 3. The scale and scope of a covered entity's cybersecurity
9 program is appropriate if the cost to operate the cybersecurity
10 program is no less than the covered entity's most recently
11 calculated maximum probable loss value.

12 4. a. A covered entity that satisfies all requirements
13 of this section is entitled to an affirmative defense to any
14 cause of action sounding in tort that is brought under the
15 laws of this state or in the courts of this state and that
16 alleges that the failure to implement reasonable information
17 security controls resulted in a data breach concerning personal
18 information or restricted information.

19 b. A covered entity satisfies all requirements of this
20 section if its cybersecurity program reasonably conforms to an
21 industry-recognized cybersecurity framework, as described in
22 section 554G.3.

23 Sec. 3. NEW SECTION. 554G.3 Cybersecurity program
24 framework.

25 1. A covered entity's cybersecurity program, as
26 described in section 554G.2, reasonably conforms to an
27 industry-recognized cybersecurity framework for purposes of
28 section 554G.2 if any of the following are true:

29 a. (1) The cybersecurity program reasonably conforms to the
30 current version of any of the following or any combination of
31 the following, subject to subparagraph (2) and subsection 2:

32 (a) The framework for improving critical infrastructure
33 cybersecurity developed by the national institute of standards
34 and technology.

35 (b) National institute of standards and technology special

1 publication 800-171.

2 (c) National institute of standards and technology special
3 publications 800-53 and 800-53a.

4 (d) The federal risk and authorization management program
5 security assessment framework.

6 (e) The center for internet security critical security
7 controls for effective cyber defense.

8 (f) The international organization for
9 standardization/international electrotechnical commission 27000
10 family — information security management systems.

11 (2) When a final revision to a framework listed in
12 subparagraph (1) is published, a covered entity whose
13 cybersecurity program reasonably conforms to that framework
14 shall reasonably conform the elements of its cybersecurity
15 program to the revised framework within the time frame provided
16 in the relevant framework upon which the covered entity intends
17 to rely to support its affirmative defense, but in no event
18 later than one year after the publication date stated in the
19 revision.

20 b. (1) The covered entity is regulated by the state, by
21 the federal government, or both, or is otherwise subject to
22 the requirements of any of the laws or regulations listed
23 below, and the cybersecurity program reasonably conforms to
24 the entirety of the current version of any of the following,
25 subject to subparagraph (2):

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

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

31 (c) The federal Information Security Modernization Act of
32 2014, Pub. L. No. 113-283.

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

35 (e) Chapter 507F.

1 (f) Any applicable rules, regulations, or guidelines for
2 critical infrastructure protection adopted by the federal
3 environmental protection agency, the federal cybersecurity
4 and infrastructure security agency, or the north American
5 reliability corporation.

6 (2) When a framework listed in subparagraph (1) is amended,
7 a covered entity whose cybersecurity program reasonably
8 conforms to that framework shall reasonably conform the
9 elements of its cybersecurity program to the amended framework
10 within the time frame provided in the relevant framework
11 upon which the covered entity intends to rely to support its
12 affirmative defense, but in no event later than one year after
13 the effective date of the amended framework.

14 c. (1) The cybersecurity program reasonably complies
15 with both the current version of the payment card industry
16 data security standard and conforms to the current version of
17 another applicable industry-recognized cybersecurity framework
18 listed in paragraph "a", subject to subparagraph (2) and
19 subsection 2.

20 (2) When a final revision to the payment card industry
21 data security standard is published, a covered entity whose
22 cybersecurity program reasonably complies with that standard
23 shall reasonably comply the elements of its cybersecurity
24 program with the revised standard within the time frame
25 provided in the relevant framework upon which the covered
26 entity intends to rely to support its affirmative defense, but
27 not later than the effective date for compliance.

28 2. If a covered entity's cybersecurity program reasonably
29 conforms to a combination of industry-recognized cybersecurity
30 frameworks, or complies with a standard, as in the case of the
31 payment card industry data security standard, as described in
32 subsection 1, paragraph "a" or "c", and two or more of those
33 frameworks are revised, the covered entity whose cybersecurity
34 program reasonably conforms to or complies with, as applicable,
35 those frameworks shall reasonably conform the elements of its

1 cybersecurity program to or comply with, as applicable, all of
2 the revised frameworks within the time frames provided in the
3 relevant frameworks but in no event later than one year after
4 the latest publication date stated in the revisions.

5 **Sec. 4. NEW SECTION. 554G.4 Causes of action.**

6 This chapter shall not be construed to provide a private
7 right of action, including a class action, with respect to any
8 act or practice regulated under this chapter.