* Drafted for discussion purposes only.

** Reflects a high-level review of Utah's data breach notification law. It does not reflect an exhaustive look at all other UT laws that may need to be reviewed to move legislation in the state.

*** Not an indication of plans to move UT-specific legislation at this point.

SAFE HARBOR FOR CYBERSECURITY PROGRAM

2019 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: ________________

[Senate/House] Sponsor:

General Description:

This bill amends §§ 13-44-102 and 13-44-301 of the Utah Code and enacts §§ 13-44-401 – 404 of the Utah Code, to provide a legal safe harbor to covered entities that implement a specified cybersecurity program.

Highlighted Provisions:

This bill:

- defines terms;
- establishes a legal safe harbor by this Act that may be pled as an affirmative defense to a cause of action sounding in statute, tort or contract that alleges or relates to the failure to implement reasonable information security controls, resulting in a breach of system security;
- establishes a safe harbor that shall apply to all covered entities that implement a cybersecurity program that meets the requirements of the Act;
- acknowledges the need to encourage businesses to achieve a higher level of cybersecurity through voluntary action;
- does not create a minimum cybersecurity standard;
- does not impose liability upon businesses that do not obtain or maintain practices in accordance with this Act.

Utah Code Sections Affected:

AMENDS:

13-44-102

13-44-301

ENACTS:

13-44-401
13-44-402
13-44-403
13-44-404

Be it enacted by the Legislature of the state of Utah:

Section 1. Section 13-44-102 is amended to read:

13-44-102. Definitions.

As used in this chapter:

(1) “Business” means any limited liability company, limited liability partnership, corporation, sole proprietorship, association, or other group, however organized and whether operating for profit or not for profit, including a financial institution organized, chartered, or holding a license authorizing operation under the laws of this state, any other state, the United States, or any other country, or the parent or subsidiary of any of the foregoing.

[~~(1)~~] (2)

(a) "Breach of system security" means an unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information.

(b) "Breach of system security" does not include the acquisition of personal information by an employee or agent of the person possessing unencrypted computerized data unless the personal information is used for an unlawful purpose or disclosed in an unauthorized manner.

(3) “Covered entity” means a person that accesses, maintains, communicates, or processes personal information in or through one or more systems, networks, or services located in or outside this state.

[~~(2)~~] (4) "Consumer" means a natural person.

(5) “Encryption” means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

[~~(3)~~] (6) "Financial institution" means the same as that term is defined in 15 U.S.C. Sec. 6809.

[~~(4)~~] (7)

(a) “Personal information” means a person’s first name or first initial and last name, combined with any one or more of the following data elements relating to that person when either the name or date element is unencrypted or not protected by another method that renders the data unreadable or unusable:

i. Social security number;

ii.

(A) Financial account number, or credit or debit card number; and

(B) Any required security code, a , access code, or password that would permit access to the person's account; or

iii. driver’s license number or state identification card number.

(b) “Personal information” does not include information regardless of its source, contained in federal, state, or local government records or in widely distributed media that are lawfully made available to the general public.

[~~(5)~~] (8) “Record” includes materials maintained in any form, including paper and electronic.

(9) “Restricted information” means any information about a consumer, other than personal information, that, alone or in combination with other information, including personal information, can be used to distinguish or trace the consumer’s identity or that is linked or linkable to a consumer, if the information is unencrypted or not protected by another method that renders the data unreadable or unusable, and the breach of which is likely to result in the misuse of personal information for identity theft or fraud purposes.

Section 2. Section 13-44-301(2) is amended to read:

(2)
~~(a)~~ Nothing in this chapter creates a private right of action.
~~(b) Nothing in this chapter affects any private right of action existing under other law, including contract or tort.~~

Section 3. Section 13-44-401 is enacted to read:

13-44-401. Cybersecurity requirements to seek affirmative defense.

(1) A covered entity seeking an affirmative defense under this chapter shall create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information or restricted information and that reasonably aligns with an industry recognized cybersecurity framework, in accordance with Section 13-44-402.

(2) A covered entity's cybersecurity program shall be designed to do all of the following with respect to the information described in Subsection (1) of this Section, as applicable:

(a) Protect the security and confidentiality of the information;

(b) Protect against any anticipated threats or hazards to the security or integrity of the information;

(c) Protect against unauthorized acquisition of the information that is likely to result in the misuse of personal information or restricted information for identity theft or fraud purposes against whom the information relates.

(3) The scale and scope of a covered entity's cybersecurity program under Subsection (1) of this Section, as applicable, is appropriate if it is based on all of the following factors:

(a) The size and complexity of the covered entity;

(b) The nature and scope of the activities of the covered entity;

(c) The sensitivity of the information to be protected;

(d) The cost and availability of tools to improve information security and reduce vulnerabilities;

(e) The resources available to the covered entity.

(4) A covered entity that satisfies Subsections (1), (2), and (3) of this Section is entitled to an affirmative defense to any cause of action sounding in statute, tort or contract that is brought by

any public or private actor under the laws or in the courts of this state or any state in which this Act has been adopted and that alleges that the failure to implement reasonable information security controls resulted in a breach of system security concerning personal information or restricted information.

Section 4. Sections 13-44-402 is enacted to read:

13-44-402. Conform to industry standard.

(1) A covered entity's cybersecurity program, as described in Section 13-44-401, reasonably aligns with an industry recognized cybersecurity framework for purposes of that Section if Subsections (2), (3), or (4) of this Section is satisfied.

(2)

(a) The cybersecurity program reasonably aligns with the current version of any of the following or any combination of the following, subject to Subsections (2)(b) and (5) of this Section:

i. The "framework for improving critical infrastructure cybersecurity" developed by the "national institute of standards and technology" (NIST);

ii. "NIST special publication 800-171";

iii. "NIST special publications 800-53 and 800-53a ";

iv. The "federal risk and authorization management program (FedRAMP) security assessment framework";

v. The "center for internet security critical security controls for effective cyber defense";

vi. The "international organization for standardization/international electrotechnical commission 27000 family - information security management systems."

(b) When a final revision to a framework listed in Subsection (2)(a) of this Section is published, a covered entity relying upon that framework for purposes of this Section shall adopt the revised framework not later than one year after the publication date stated in the revision.

(3)

(a) The covered entity is regulated by the state, by the federal government, or both, or is otherwise subject to the requirements of any of the laws or regulations listed below, and the cybersecurity program reasonably aligns with the entirety of the current version of any of the following, subject to Subsection (3)(b) of this Section:

i. The security requirements of the "Health Insurance Portability and Accountability Act of 1996," as set forth in 45 CFR Part 164 Subpart C;
ii. Title V of the "Gramm-Leach-Bliley Act of 1999," Public Law 106-102, as amended;
iii. The "Federal Information Security Modernization Act of 2014," Public Law 113-283;
iv. The "Health Information Technology for Economic and Clinical Health Act," as set forth in 45 CFR part 162.

(b) When a framework listed in Subsection (3)(a) of this Section is amended, a covered entity whose cybersecurity program is relying upon that framework for purposes of this Section shall adopt the amended framework not later than one year after the effective date of the amended framework.

(4)

(a) The cybersecurity program reasonably aligns with both the current version of the "payment card industry (PCI) data security standard" and the current version of another applicable industry recognized cybersecurity framework listed in Subsection (2) of this Section, subject to Subsections (4)(b) and (5) of this Section.

(b) When a final revision to the "PCI data security standard" is published, a covered entity whose cybersecurity program relies upon that standard for purposes of this Section shall adopt the revised standard not later than one year after the publication date stated in the revision.

(5) If a covered entity's cybersecurity program reasonably aligns with a combination of industry recognized cybersecurity frameworks or with a standard, as in the case of the PCI data security standard, as described in Subsections (2) or (4) of this Section, and two or more of those frameworks are revised, the covered entity whose cybersecurity program is reliant upon those frameworks for purposes of this Section shall adopt all of the revised frameworks not later than one year after the latest publication date stated in the revisions.

Section 5. Sections 13-44-403 is enacted to read:

13-44-403. Limitation of cause of action.

This chapter shall not be construed to provide a cause of action to any public or private entity or consumers, including a class action, with respect to any act or practice regulated under this chapter.

Section 6. Sections 13-44-404 is enacted to read:

13-44-404. Severability.

If any provision of this chapter or its application to a covered entity is for any reason held to be invalid, the remainder of the provisions under those sections and the application of such provisions to other covered entities shall not be thereby affected.