LEGISLATIVE GENERAL COUNSEL
₵ Approved for Filing: S. Elder ₵
₵ 01-15-24 4:15 PM ₵

ONLINE DATA SECURITY AND PRIVACY AMENDMENTS

2024 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Wayne A. Harper

House Sponsor: _____

LONG TITLE

General Description:

This bill amends provisions related to cybersecurity, breach notification requirements, and authorized domain name extensions.

Highlighted Provisions:

This bill:

- defines terms;
- makes technical and conforming changes;
- grants rulemaking authority to the Utah Cyber Center to define:
  - a person's breach notification responsibilities; and
  - a governmental entity's reporting responsibilities to the Utah Cyber Center; and
- requires governmental entities to use authorized domain name extensions for websites and email.

Money Appropriated in this Bill:

None

Other Special Clauses:

None

Utah Code Sections Affected:

AMENDS:

13-44-202, as last amended by Laws of Utah 2023, Chapter 496

63A-16-501, as last amended by Laws of Utah 2022, Chapter 169

S.B. 98

63A-16-510, as enacted by Laws of Utah 2023, Chapter 496

63A-16-511, as enacted by Laws of Utah 2023, Chapter 496

63D-2-102, as last amended by Laws of Utah 2023, Chapter 275

63D-2-105, as enacted by Laws of Utah 2023, Chapter 496

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

Section 1. Section **13-44-202** is amended to read:

13-44-202. Personal information -- Disclosure of system security breach.

(1) (a) A person who owns or licenses computerized data that includes personal information concerning a Utah resident shall, when the person becomes aware of a breach of system security, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused for identity theft or fraud purposes.

(b) If an investigation under Subsection (1)(a) reveals that the misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur, the person shall provide notification to each affected Utah resident.

(c) If an investigation under Subsection (1)(a) reveals that the misuse of personal information relating to 500 or more Utah residents, for identity theft or fraud purposes, has occurred or is reasonably likely to occur, the person shall, in addition to the notification required in Subsection (1)(b), provide notification to:

(i) the Office of the Attorney General; and

(ii) the Utah Cyber Center created in Section 63A-16-510.

(d) If an investigation under Subsection (1)(a) reveals that the misuse of personal information relating to 1,000 or more Utah residents, for identity theft or fraud purposes, has occurred or is reasonably likely to occur, the person shall, in addition to the notification required in Subsections (1)(b) and (c), provide notification to each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, as defined in 15 U.S.C. Sec. 1681a.

(2) A person required to provide notification under Subsection (1) shall provide the notification in the most expedient time possible without unreasonable delay:

(a) considering legitimate investigative needs of law enforcement, as provided in

Subsection (4)(a);

(b) after determining the scope of the breach of system security; and

(c) after restoring the reasonable integrity of the system.

(3) (a) A person who maintains computerized data that includes personal information that the person does not own or license shall notify and cooperate with the owner or licensee of the information of any breach of system security immediately following the person's discovery of the breach if misuse of the personal information occurs or is reasonably likely to occur.

(b) Cooperation under Subsection (3)(a) includes sharing information relevant to the breach with the owner or licensee of the information.

(4) (a) Notwithstanding Subsection (2), a person may delay providing notification under Subsection (1)(b) at the request of a law enforcement agency that determines that notification may impede a criminal investigation.

(b) A person who delays providing notification under Subsection (4)(a) shall provide notification in good faith without unreasonable delay in the most expedient time possible after the law enforcement agency informs the person that notification will no longer impede the criminal investigation.

(5) (a) A notification required by Subsection (1)(b) may be provided:

(i) in writing by first-class mail to the most recent address the person has for the resident;

(ii) electronically, if the person's primary method of communication with the resident is by electronic means, or if provided in accordance with the consumer disclosure provisions of 15 U.S.C. Section 7001;

(iii) by telephone, including through the use of automatic dialing technology not prohibited by other law; or

(iv) for residents of the state for whom notification in a manner described in Subsections (5)(a)(i) through (iii) is not feasible, by publishing notice of the breach of system security:

(A) in a newspaper of general circulation; and

(B) as required in Section 45-1-101.

(b) If a person maintains the person's own notification procedures as part of an information security policy for the treatment of personal information the person is considered

to be in compliance with the notification requirement in Subsection (1)(b) if the procedures are otherwise consistent with this chapter's timing requirements and the person notifies each affected Utah resident in accordance with the person's information security policy in the event of a breach.

(c) A person who is regulated by state or federal law and maintains procedures for a breach of system security under applicable law established by the primary state or federal regulator is considered to be in compliance with this part if the person notifies each affected Utah resident in accordance with the other applicable law in the event of a breach.

(6) (a) If a person providing a notification under Subsection (1)(c) to the Office of the Attorney General or the Utah Cyber Center submits the information required under Subsection 63G-2-309(1)(a)(i), records submitted to the Office of the Attorney General or the Utah Cyber Center under Subsection (1)(c) and information produced by the Office of the Attorney General or the Utah Cyber Center for any coordination or assistance provided to the person are presumed to be confidential and are a protected record under Subsections 63G-2-305(1) and (2).

(b) The [~~department~~] Office of the Attorney General or the Utah Cyber Center may disclose information provided by a person under Subsection (1)(c) or produced as described in Subsection (6)(a) only if:

(i) disclosure is necessary to prevent imminent and substantial harm; or

(ii) the information is anonymized or aggregated in a manner that makes it unlikely that information that is a trade secret, as defined in Section 13-24-2, will be disclosed.

(7) A waiver of this section is contrary to public policy and is void and unenforceable.

(8) In accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act, the Utah Cyber Center shall make rules to define a person's notification responsibilities under this section.

Section 2. Section **63A-16-501** is amended to read:

63A-16-501. Definitions.

As used in this part:

(1) "Breach of system security" means the unauthorized access, acquisition, disclosure, loss of access, or destruction of:

(a) personal data; or

(b) data that compromises the security, confidentiality, availability, or integrity of the computer systems used or information maintained by the governmental entity.

(2) "Center" means the Utah Geospatial Resource Center created in Section 63A-16-505.

[~~(2)~~] (3) "Database" means the State Geographic Information Database created in Section 63A-16-506.

[~~(3)~~] (4) "Geographic Information System" or "GIS" means a computer driven data integration and map production system that interrelates disparate layers of data to specific geographic locations.

(5) "Personal data" means information that is linked or can be reasonably linked to an identified individual or an identifiable individual.

[~~(4)~~] (6) "State Geographic Information Database" means the database created in Section 63A-16-506.

[~~(5)~~] (7) "Statewide Global Positioning Reference Network" or "network" means the network created in Section 63A-16-508.

Section 3. Section **63A-16-510** is amended to read:

63A-16-510. Utah Cyber Center -- Creation -- Duties.

(1) As used in this section:

(a) "Governmental entity" means the same as that term is defined in Section 63G-2-103.

(b) "Utah Cyber Center" means the Utah Cyber Center created in this section.

(2) (a) There is created within the division the Utah Cyber Center.

(b) The chief information security officer appointed under Section 63A-16-210 shall serve as the director of the Utah Cyber Center.

(3) The division shall operate the Utah Cyber Center in partnership with the following entities within the Department of Public Safety created in Section 53-1-103:

(a) the Statewide Information and Analysis Center;

(b) the State Bureau of Investigation created in Section 53-10-301; and

(c) the Division of Emergency Management created in Section 53-2a-103.

(4) In addition to the entities described in Subsection (3), the Utah Cyber Center shall collaborate with:

(a) the Cybersecurity Commission created in Section 63C-27-201;

(b) the Office of the Attorney General;

(c) the Utah Education and Telehealth Network created in Section 53B-17-105;

(d) appropriate federal partners, including the Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency;

(e) appropriate information sharing and analysis centers;

(f) [~~associations representing political subdivisions in the state, including the Utah League of Cities and Towns and the Utah Association of Counties~~] information technology directors, cybersecurity professionals, or equivalent individuals representing political subdivisions in the state; and

(g) any other person the division believes is necessary to carry out the duties described in Subsection (5).

(5) The Utah Cyber Center shall, within legislative appropriations:

(a) by June 30, 2024, develop a statewide strategic cybersecurity plan for executive branch agencies and other governmental entities;

(b) with respect to executive branch agencies:

(i) identify, analyze, and, when appropriate, mitigate cyber threats and vulnerabilities;

(ii) coordinate cybersecurity resilience planning;

(iii) provide cybersecurity incident response capabilities; and

(iv) recommend to the division standards, policies, or procedures to increase the cyber resilience of executive branch agencies individually or collectively;

(c) at the request of a governmental entity, coordinate cybersecurity incident response for an incident affecting the governmental entity in accordance with Section 63A-16-511;

(d) promote cybersecurity best practices;

(e) share cyber threat intelligence with governmental entities and, through the Statewide Information and Analysis Center, with other public and private sector organizations;

(f) serve as the state cybersecurity incident response hotline to receive reports of breaches of system security, including notification or disclosure under Section 13-44-202 or 63A-16-511;

(g) develop incident response plans to coordinate federal, state, local, and private sector activities and manage the risks associated with an attack or malfunction of critical

information technology systems within the state;

(h) coordinate, develop, and share best practices for cybersecurity resilience in the state;

(i) identify sources of funding to make cybersecurity improvements throughout the state;

(j) develop a sharing platform to provide resources based on information, recommendations, and best practices; and

(k) partner with institutions of higher education and other public and private sector organizations to increase the state's cyber resilience.

Section 4. Section **63A-16-511** is amended to read:

63A-16-511. Reporting to the Utah Cyber Center -- Assistance to governmental entities -- Records.

(1) As used in this section:

(a) "Governmental entity" means the same as that term is defined in Section 63G-2-103.

(b) "Utah Cyber Center" means the Utah Cyber Center created in Section 63A-16-510.

(2) A governmental entity shall contact the Utah Cyber Center as soon as practicable when the governmental entity becomes aware of a breach of system security.

(3) The Utah Cyber Center shall provide the governmental entity with assistance in responding to the breach of system security, which may include:

(a) conducting all or part of the investigation required under Subsection 13-44-202(1)(a);

(b) assisting law enforcement with the law enforcement investigation if needed;

(c) determining the scope of the breach of system security;

(d) assisting the governmental entity in restoring the reasonable integrity of the system; or

(e) providing any other assistance in response to the reported breach of system security.

(4) (a) A person providing information to the Utah Cyber Center may submit the information required in Section 63G-2-309 to request that the information submitted by the person and information produced by the Utah Cyber Center in the course of the Utah Cyber Center's investigation be classified as a confidential protected record.

(b) Information submitted to the Utah Cyber Center under Subsection 13-44-202(1)(c) regarding a breach of system security may include information regarding the type of breach, the attack vector, attacker, indicators of compromise, and other details of the breach that are requested by the Utah Cyber Center.

(c) A governmental entity that is required to submit information under Section 63A-16-511 shall provide records to the Utah Cyber Center as a shared record in accordance with Section 63G-2-206.

(5) In accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act, the Utah Cyber Center shall make rules to define reporting responsibilities for governmental entities under this section.

Section 5. Section **63D-2-102** is amended to read:

63D-2-102. Definitions.

As used in this chapter:

(1) (a) "Collect" means the gathering of personally identifiable information:

(i) from a user of a governmental website; or

(ii) about a user of the governmental website.

(b) "Collect" includes use of any identifying code linked to a user of a governmental website.

(2) "Court website" means a website on the Internet that is operated by or on behalf of any court created in Title 78A, Chapter 1, Judiciary.

(3) "Governmental entity" means:

(a) an executive branch agency as defined in Section 63A-16-102;

(b) the legislative branch;

(c) the judicial branch;

(d) the State Board of Education created in Section 20A-14-101.5;

(e) the Utah Board of Higher Education created in Section 53B-1-402;

(f) an institution of higher education as defined in Section 53B-1-102; and

(g) a political subdivision of the state:

(i) as defined in Section 17B-1-102; and

(ii) including a school district created under Section 53G-3-301 or 53G-3-302.

(4) (a) "Governmental website" means a website on the Internet that is operated by or

on behalf of a governmental entity.

(b) "Governmental website" includes a court website.

(5) "Governmental website operator" means a governmental entity or person acting on behalf of the governmental entity that:

(a) operates a governmental website; and

(b) collects or maintains personally identifiable information from or about a user of that website.

(6) "Personally identifiable information" means information that identifies:

(a) a user by:

(i) name;

(ii) account number;

(iii) physical address;

(iv) email address;

(v) telephone number;

(vi) Social Security number;

(vii) credit card information; or

(viii) bank account information;

(b) a user as having requested or obtained specific materials or services from a governmental website;

(c) Internet sites visited by a user; or

(d) any of the contents of a user's data-storage device.

(7) "School" means a public or private elementary or secondary school.

[~~(7)~~] (8) "User" means a person who accesses a governmental website.

Section 6. Section **63D-2-105** is amended to read:

63D-2-105. Use of authorized domain extensions for government websites.

(1) [~~(a)~~] As used in this section, "authorized top level domain" means any of the following suffixes that follows the domain name in a website address:

[~~(i)~~] (a) gov;

[~~(ii)~~] (b) edu; and

[~~(iii)~~] (c) mil.

(2) Beginning [~~January~~] July 1, 2025, a governmental entity shall use an authorized top

level domain for:

(a) the website address for the governmental entity's government website; and

(b) the email addresses used by the governmental entity and the governmental entity's employees.

(3) Notwithstanding Subsection (2), a governmental entity may operate a website that uses a top level domain that is not an authorized top level domain if:

(a) (i) a reasonable person would not mistake the website as the governmental entity's primary website; and

[~~(b)~~] (ii) the governmental website is:

[~~(i)~~] (A) solely for internal use and not intended for use by members of the public;

[~~(ii)~~] (B) temporary and in use by the governmental entity for a period of less than one year; or

[~~(iii)~~] (C) related to an event, program, or informational campaign operated by the governmental entity in partnership with another person that is not a governmental entity[.]; or

(b) the governmental entity is a school district or a school that is not an institution of higher education and the use of an authorized top level domain is otherwise prohibited, provided that once the use of an authorized top level domain is not otherwise prohibited, the school district or school shall transition to an authorized top level domain within 15 months.

(4) The chief information officer appointed under Section 63A-16-201 may authorize a waiver of the requirement in Subsection (2) if:

(a) there are extraordinary circumstances under which use of an authorized domain extension would cause demonstrable harm to citizens or businesses; and

(b) the executive director or chief executive of the governmental entity submits a written request to the chief information officer that includes a justification for the waiver.

Section 7. **Effective date.**

This bill takes effect on May 1, 2024.