**13-44-202**, as last amended by Laws of Utah 2019, Chapter 348

ENACTS:

**63A-16-302.1**, Utah Code Annotated 1953

**63A-16-510**, Utah Code Annotated 1953

**63A-16-511**, Utah Code Annotated 1953

**63D-2-105**, Utah Code Annotated 1953

---

*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 **Ĥ→ [~~:~~] each affected Utah resident. ←Ĥ**

**Ĥ→ [~~(i) each affected Utah resident[.];~~**

**~~(ii) the Office of the Attorney General; and~~**

**~~(iii) the Utah Cyber Center created in Section 62A-16-510.~~]**

**(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 62A-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. ←Ĥ**

(2) A person required to provide notification under Subsection (1) shall provide the

(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) Ĥ→ [~~(i)~~] ←Ĥ 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 [~~this section~~] Subsection (1)(b) Ĥ→ [~~(i)~~] ←Ĥ 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 [~~this chapter's notification requirements~~] the notification requirement in Subsection (1)(b) Ĥ→ [~~(i)~~] ←Ĥ 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.

**Ĥ→ (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 Section 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 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. ←Ĥ**

**Ĥ→ [~~(6)~~] (7) ←Ĥ** A waiver of this section is contrary to public policy and is void and unenforceable.

Section 2. Section **63A-16-302.1** is enacted to read:

**63A-16-302.1. Reporting on consolidation of certain information technology services.**

(1) The division shall, in collaboration with the Cybersecurity Commission created in Section 63C-27-201, identify opportunities, limitations, and barriers to enhancing the overall cybersecurity resilience of the state by consolidating:

(a) certain information technology services utilized by governmental entities; and

(b) to the extent feasible, the information technology networks that are operated or utilized by governmental entities.

(2) On or before November 15, 2023, the division shall report the information described in Subsection (1) to:

(a) the Government Operations Interim Committee;

(b) the Infrastructure and General Government Appropriations Subcommittee; and

(c) the Cybersecurity Commission created in Section 63C-27-201.

Section 3. Section **63A-16-510** is enacted 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.

collaborate with:

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

(b) the Office of the Attorney General;

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

**Ŝ→ [~~(c)~~] (d) ←Ŝ** appropriate federal partners, including the Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency;

**Ŝ→ [~~(d)~~] (e) ←Ŝ** appropriate information sharing and analysis centers;

**Ŝ→ [~~(e)~~] (f) ←Ŝ** associations representing political subdivisions in the state, including the Utah League of Cities and Towns and the Utah Association of Counties; and

**Ŝ→ [~~(f)~~] (g) ←Ŝ** 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