

**CYBERSECURITY AMENDMENTS**

2023 GENERAL SESSION

STATE OF UTAH

**Chief Sponsor: Wayne A. Harper**

House Sponsor: Jefferson S. Burton

---

**LONG TITLE**

**General Description:**

This bill enacts provisions relating to cybersecurity.

**Highlighted Provisions:**

This bill:

- ▶ amends the disclosure requirement for system security breaches;
- ▶ requires the Division of Technology Services to report certain information regarding consolidation of networks used by governmental entities;
- ▶ creates the Utah Cyber Center and defines the center's duties;
- ▶ requires governmental entities in the state to report a breach of system security to the Utah Cyber Center; and
- ▶ requires governmental websites to use an authorized top level domain by January 1, 2025.

**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 2019, Chapter 348

ENACTS:

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

29 [63A-16-510](#), Utah Code Annotated 1953

30 [63A-16-511](#), Utah Code Annotated 1953

31 [63D-2-105](#), Utah Code Annotated 1953

32 

---

---

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

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

35 **13-44-202. Personal information -- Disclosure of system security breach.**

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

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

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

- 49 (i) the Office of the Attorney General; and
- 50 (ii) the Utah Cyber Center created in Section [62A-16-510](#).

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

56 Sec. 1681a.

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

59 (a) considering legitimate investigative needs of law enforcement, as provided in  
60 Subsection (4)(a);

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

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

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

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

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

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

76 (5) (a) A notification required by [~~this section~~] Subsection (1)(b) may be provided:

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

79 (ii) electronically, if the person's primary method of communication with the resident is  
80 by electronic means, or if provided in accordance with the consumer disclosure provisions of  
81 15 U.S.C. Section 7001;

82 (iii) by telephone, including through the use of automatic dialing technology not

83 prohibited by other law; or

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

87 (A) in a newspaper of general circulation; and

88 (B) as required in Section [45-1-101](#).

89 (b) If a person maintains the person's own notification procedures as part of an  
90 information security policy for the treatment of personal information the person is considered  
91 to be in compliance with ~~[this chapter's notification requirements]~~ the notification requirement  
92 in Subsection (1)(b) if the procedures are otherwise consistent with this chapter's timing  
93 requirements and the person notifies each affected Utah resident in accordance with the  
94 person's information security policy in the event of a breach.

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

99 (6) (a) If a person providing a notification under Subsection (1)(c) to the Office of the  
100 Attorney General or the Utah Cyber Center submits the information required under Subsection  
101 [63G-2-309\(1\)\(a\)\(i\)](#), records submitted to the Office of the Attorney General or the Utah Cyber  
102 Center under Subsection (1)(c) and information produced by the Office of the Attorney General  
103 or the Utah Cyber Center for any coordination or assistance provided to the person are  
104 presumed to be confidential and are a protected record under Subsections [63G-2-305\(1\)](#) and  
105 (2).

106 (b) The department may disclose information provided by a person under Subsection  
107 (1)(c) or produced as described in Subsection (6)(a) only if:

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

109 (ii) the information is anonymized or aggregated in a manner that makes it unlikely that

110 information that is a trade secret, as defined in Section 13-24-2, will be disclosed.

111 ~~[(6)]~~ (7) A waiver of this section is contrary to public policy and is void and  
112 unenforceable.

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

114 **63A-16-302.1. Reporting on consolidation of certain information technology**  
115 **services.**

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

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

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

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

124 (a) the Government Operations Interim Committee;

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

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

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

128 **63A-16-510. Utah Cyber Center -- Creation -- Duties.**

129 (1) As used in this section:

130 (a) "Governmental entity" means the same as that term is defined in Section  
131 63G-2-103.

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

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

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

136 (3) The division shall operate the Utah Cyber Center in partnership with the following

137 entities within the Department of Public Safety:  
138       (a) the Statewide Information and Analysis Center;  
139       (b) the State Bureau of Investigation; and  
140       (c) the Division of Emergency Management.  
141       (4) In addition to the entities described in Subsection (3), the Utah Cyber Center shall  
142 collaborate with:  
143       (a) the Cybersecurity Commission created in Section [63C-27-201](#);  
144       (b) the Office of the Attorney General;  
145       (c) the Utah Education and Telehealth Network created in Section [53B-17-105](#);  
146       (d) appropriate federal partners, including the Federal Bureau of Investigation and the  
147 Cybersecurity and Infrastructure Security Agency;  
148       (e) appropriate information sharing and analysis centers;  
149       (f) associations representing political subdivisions in the state, including the Utah  
150 League of Cities and Towns and the Utah Association of Counties; and  
151       (g) any other person the division believes is necessary to carry out the duties described  
152 in Subsection (5).  
153       (5) The Utah Cyber Center shall, within legislative appropriations:  
154       (a) by June 30, 2024, develop a statewide strategic cybersecurity plan for executive  
155 branch agencies and other governmental entities;  
156       (b) with respect to executive branch agencies:  
157       (i) identify, analyze, and, when appropriate, mitigate cyber threats and vulnerabilities;  
158       (ii) coordinate cybersecurity resilience planning;  
159       (iii) provide cybersecurity incident response capabilities; and  
160       (iv) recommend to the division standards, policies, or procedures to increase the cyber  
161 resilience of executive branch agencies individually or collectively;  
162       (c) at the request of a governmental entity, coordinate cybersecurity incident response  
163 for an incident affecting the governmental entity in accordance with Section [63A-16-511](#);

- 164 (d) promote cybersecurity best practices;
- 165 (e) share cyber threat intelligence with governmental entities and, through the
- 166 Statewide Information and Analysis Center, with other public and private sector organizations;
- 167 (f) serve as the state cybersecurity incident response hotline to receive reports of
- 168 breaches of system security, including notification or disclosure under Section [13-44-202](#) or
- 169 [63A-16-511](#);
- 170 (g) develop incident response plans to coordinate federal, state, local, and private
- 171 sector activities and manage the risks associated with an attack or malfunction of critical
- 172 information technology systems within the state;
- 173 (h) coordinate, develop, and share best practices for cybersecurity resilience in the
- 174 state;
- 175 (i) identify sources of funding to make cybersecurity improvements throughout the
- 176 state;
- 177 (j) develop a sharing platform to provide resources based on information,
- 178 recommendations, and best practices; and
- 179 (k) partner with institutions of higher education and other public and private sector
- 180 organizations to increase the state's cyber resilience.

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

182 **63A-16-511. Reporting to the Utah Cyber Center -- Assistance to governmental**

183 **entities -- Records.**

184 (1) As used in this section:

- 185 (a) "Governmental entity" means the same as that term is defined in Section
- 186 [63G-2-103](#).
- 187 (b) "Utah Cyber Center" means the Utah Cyber Center created in Section [62A-16-510](#).
- 188 (2) A governmental entity shall contact the Utah Cyber Center as soon as practicable
- 189 when the governmental entity becomes aware of a breach of system security.
- 190 (3) The Utah Cyber Center shall provide the governmental entity with assistance in

191 responding to the breach of system security, which may include:

192 (a) conducting all or part of the investigation required under Subsection

193 13-44-202(1)(a);

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

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

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

197 or

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

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

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

207 (c) A governmental entity that is required to submit information under Section  
208 63A-16-511 shall provide records to the Utah Cyber Center as a shared record in accordance  
209 with Section 63G-2-206.

210 Section 5. Section **63D-2-105** is enacted to read:

211 **63D-2-105. Use of authorized domain extensions for government websites.**

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

214 (i) gov;

215 (ii) edu; and

216 (iii) mil.

217 (2) Beginning January 1, 2025, a governmental entity shall use an authorized top level



218 domain for:

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

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

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

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

226 (b) the governmental website is:

227 (i) solely for internal use and not intended for use by members of the public;

228 (ii) temporary and in use by the governmental entity for a period of less than one year;

229 or

230 (iii) related to an event, program, or informational campaign operated by the

231 governmental entity in partnership with another person that is not a governmental entity.

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

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

236 (b) the executive director or chief executive of the governmental entity submits a

237 written request to the chief information officer that includes a justification for the waiver.