

Senator Wayne A. Harper proposes the following substitute bill:

ONLINE DATA SECURITY AND PRIVACY AMENDMENTS

2024 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Wayne A. Harper

House Sponsor: Jefferson S. Burton

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;
- ▶ describes a person's breach notification responsibilities to the Utah Cyber Center;

and

- ▶ describes a governmental entity's reporting responsibilities to the Utah Cyber Center.

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



26 [63D-2-102](#), as last amended by Laws of Utah 2023, Chapter 275

27 [63D-2-105](#), as enacted by Laws of Utah 2023, Chapter 496

28 ENACTS:

29 [63A-16-1101](#), Utah Code Annotated 1953

30 RENUMBERS AND AMENDS:

31 [63A-16-1102](#), (Renumbered from 63A-16-510, as enacted by Laws of Utah 2023,
32 Chapter 496)

33 [63A-16-1103](#), (Renumbered from 63A-16-511, as enacted by Laws of Utah 2023,
34 Chapter 496)



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

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

38 **13-44-202. Personal information -- Disclosure of system security breach.**

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

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

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

- 51 (i) the Office of the Attorney General; and
- 52 (ii) the Utah Cyber Center created in Section [~~63A-16-510~~] [63A-16-1102](#).

53 (d) If an investigation under Subsection (1)(a) reveals that the misuse of personal
54 information relating to 1,000 or more Utah residents, for identity theft or fraud purposes, has
55 occurred or is reasonably likely to occur, the person shall, in addition to the notification
56 required in Subsections (1)(b) and (c), provide notification to each consumer reporting agency

57 that compiles and maintains files on consumers on a nationwide basis, as defined in 15 U.S.C.
58 Sec. 1681a.

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

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

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

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

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

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

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

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

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

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

81 (ii) electronically, if the person's primary method of communication with the resident is
82 by electronic means, or if provided in accordance with the consumer disclosure provisions of
83 15 U.S.C. Section 7001;

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

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

88 security:

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

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

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

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

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

108 (b) A person providing notification under Subsection (1)(c) to the Office of the
109 Attorney General or the Utah Cyber Center of a breach of system security shall include the
110 following information in the notification:

111 (i) the date the breach of system security occurred;

112 (ii) the date the breach of system security was discovered;

113 (iii) the total number of people affected by the breach of system security, including the
114 total number of Utah residents affected;

115 (iv) the type of personal information involved in the breach of system security; and

116 (v) a short description of the breach of system security that occurred.

117 ~~(b)~~ (c) The ~~[department]~~ Office of the Attorney General or the Utah Cyber Center
118 may disclose information provided by a person under Subsection (1)(c) or produced as

119 described in Subsection (6)(a) only if:

- 120 (i) disclosure is necessary to prevent imminent and substantial harm; or
 121 (ii) the information is anonymized or aggregated in a manner that makes it unlikely that
 122 information that is a trade secret, as defined in Section [13-24-2](#), will be disclosed.

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

124 Section 2. Section **63A-16-1101** is enacted to read:

125 **Part 11. Utah Cyber Center**

126 **63A-16-1101. Definitions.**

127 As used in this part:

128 (1) "Cyber Center" means the Utah Cyber Center created in Section [63A-16-1102](#).

129 (2) "Data breach" means the unauthorized access, acquisition, disclosure, loss of
 130 access, or destruction of:

131 (a) personal data; or

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

134 (3) "Governmental entity" means the same as that term is defined in Section
 135 [63G-2-103](#).

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

138 Section 3. Section **63A-16-1102**, which is renumbered from Section 63A-16-510 is
 139 renumbered and amended to read:

140 ~~**[63A-16-510].**~~ **63A-16-1102. Utah Cyber Center -- Creation -- Duties.**

141 ~~[(1) As used in this section:]~~

142 ~~[(a) "Governmental entity" means the same as that term is defined in Section
 143 [63G-2-103](#).]~~

144 ~~[(b) "Utah Cyber Center" means the Utah Cyber Center created in this section.]~~

145 ~~[(2)]~~ (1) (a) There is created within the division the Utah Cyber Center.

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

148 ~~[(3)]~~ (2) The division shall operate the [~~Utah~~] Cyber Center in partnership with the
 149 following entities within the Department of Public Safety created in Section [53-1-103](#):

- 150 (a) the Statewide Information and Analysis Center;
- 151 (b) the State Bureau of Investigation created in Section 53-10-301; and
- 152 (c) the Division of Emergency Management created in Section 53-2a-103.
- 153 ~~[(4)]~~ (3) In addition to the entities described in Subsection (3), the ~~[Utah]~~ Cyber Center
- 154 shall collaborate with:
- 155 (a) the Cybersecurity Commission created in Section 63C-27-201;
- 156 (b) the Office of the Attorney General;
- 157 (c) the Utah Education and Telehealth Network created in Section 53B-17-105;
- 158 (d) appropriate federal partners, including the Federal Bureau of Investigation and the
- 159 Cybersecurity and Infrastructure Security Agency;
- 160 (e) appropriate information sharing and analysis centers;
- 161 (f) ~~[associations representing political subdivisions in the state, including the Utah~~
- 162 ~~League of Cities and Towns and the Utah Association of Counties]~~ information technology
- 163 directors, cybersecurity professionals, or equivalent individuals representing political
- 164 subdivisions in the state; and
- 165 (g) any other person the division believes is necessary to carry out the duties described
- 166 in Subsection ~~[(5)]~~ (4).
- 167 ~~[(5)]~~ (4) The ~~[Utah]~~ Cyber Center shall, within legislative appropriations:
- 168 (a) by June 30, 2024, develop a statewide strategic cybersecurity plan for ~~[executive~~
- 169 ~~branch agencies and other]~~ governmental entities;
- 170 (b) with respect to executive branch agencies:
- 171 (i) identify, analyze, and, when appropriate, mitigate cyber threats and vulnerabilities;
- 172 (ii) coordinate cybersecurity resilience planning;
- 173 (iii) provide cybersecurity incident response capabilities; and
- 174 (iv) recommend to the division standards, policies, or procedures to increase the cyber
- 175 resilience of executive branch agencies individually or collectively;
- 176 (c) at the request of a governmental entity, coordinate cybersecurity incident response
- 177 for ~~[an incident]~~ a data breach affecting the governmental entity in accordance with Section
- 178 ~~[63A-16-5H]~~ 63A-16-1103;
- 179 (d) promote cybersecurity best practices;
- 180 (e) share cyber threat intelligence with governmental entities and, through the

181 Statewide Information and Analysis Center, with other public and private sector organizations;

182 (f) serve as the state cybersecurity incident response [~~hotline~~] repository to receive
183 reports of breaches of system security, including notification or disclosure under Section
184 13-44-202 [~~or 63A-16-511~~] and data breaches under Section 63A-16-1103;

185 (g) develop incident response plans to coordinate federal, state, local, and private
186 sector activities and manage the risks associated with an attack or malfunction of critical
187 information technology systems within the state;

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

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

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

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

196 Section 4. Section **63A-16-1103**, which is renumbered from Section 63A-16-511 is
197 renumbered and amended to read:

198 ~~[63A-16-511]~~. **63A-16-1103. Reporting to the Cyber Center -- Assistance to**
199 **governmental entities -- Records.**

200 [~~(1) As used in this section:~~]

201 [~~(a) "Governmental entity" means the same as that term is defined in Section~~
202 ~~63G-2-103.~~]

203 [~~(b) "Utah Cyber Center" means the Utah Cyber Center created in Section~~
204 ~~63A-16-510.~~]

205 [~~(2)~~] (1) (a) A governmental entity shall [~~contact~~] notify the [~~Utah~~] Cyber Center as
206 soon as practicable when the governmental entity becomes aware of a data breach [~~of system~~
207 ~~security~~].

208 (b) When a governmental entity notifies the Cyber Center of a data breach under
209 Subsection (1)(a), the governmental entity shall include the following information:

210 (i) the date the data breach occurred;

211 (ii) the date the data breach was discovered;

212 (iii) the total number of people affected by the data breach, including the total number
213 of Utah residents affected;

214 (iv) the type of personal data involved in the data breach;

215 (v) a short description of the data breach that occurred;

216 (vi) the path or means by which access was gained to the system, computer, or
217 network, if known;

218 (vii) the individual or entity who perpetrated the data breach, if known; and

219 (viii) any other details requested by the Cyber Center.

220 ~~[(3)]~~ (2) The ~~[Utah]~~ Cyber Center shall provide the governmental entity with assistance
221 in responding to the data breach ~~[of system security]~~, which may include:

222 (a) conducting all or part of ~~[the]~~ an internal investigation ~~[required under Subsection~~
223 ~~13-44-202(1)(a)]~~ into the data breach;

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

225 (c) determining the scope of the data breach ~~[of system security]~~;

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

227 or

228 (e) providing any other assistance in response to the reported data breach ~~[of system~~
229 ~~security]~~.

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

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

238 ~~[(c)]~~ (3) (a) A governmental entity that is required to submit information under Section
239 ~~[63A-16-511]~~ 63A-16-1103 shall provide records to the ~~[Utah]~~ Cyber Center as a shared record
240 in accordance with Section 63G-2-206.

241 (b) The information provided to the Cyber Center by a governmental entity, and any
242 information produced by the Cyber Center in the course of the Cyber Center's investigation,

243 shall be protected and may not be disclosed.

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

245 **63D-2-102. Definitions.**

246 As used in this chapter:

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

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

249 (ii) about a user of the governmental website.

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

251 website.

252 (2) "Court website" means a website on the Internet that is operated by or on behalf of

253 any court created in Title 78A, Chapter 1, Judiciary.

254 (3) "Governmental entity" means:

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

256 (b) the legislative branch;

257 (c) the judicial branch;

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

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

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

261 (g) a political subdivision of the state:

262 (i) as defined in Section [17B-1-102](#); and

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

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

265 on behalf of a governmental entity.

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

267 (5) "Governmental website operator" means a governmental entity or person acting on

268 behalf of the governmental entity that:

269 (a) operates a governmental website; and

270 (b) collects or maintains personally identifiable information from or about a user of

271 that website.

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

273 (a) a user by:

- 274 (i) name;
- 275 (ii) account number;
- 276 (iii) physical address;
- 277 (iv) email address;
- 278 (v) telephone number;
- 279 (vi) Social Security number;
- 280 (vii) credit card information; or
- 281 (viii) bank account information;
- 282 (b) a user as having requested or obtained specific materials or services from a
- 283 governmental website;
- 284 (c) Internet sites visited by a user; or
- 285 (d) any of the contents of a user's data-storage device.

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

287 [~~(7)~~] (8) "User" means a person who accesses a governmental website.

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

289 **63D-2-105. Use of authorized domain extensions for government websites.**

290 (1) [~~(a)~~] As used in this section, "authorized top level domain" means any of the

291 following suffixes that follows the domain name in a website address:

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

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

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

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

296 level domain for:

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

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

299 employees.

300 (3) Notwithstanding Subsection (2), a governmental entity may operate a website that

301 uses a top level domain that is not an authorized top level domain if:

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

303 primary website; and

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

305 [(i)] (A) solely for internal use and not intended for use by members of the public;
306 [(ii)] (B) temporary and in use by the governmental entity for a period of less than one
307 year; or

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

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

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

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

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

320 Section 7. **Effective date.**

321 This bill takes effect on May 1, 2024.