

Privacy and Cybersecurity Amendments

2026 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Wayne A. Harper

House Sponsor:

LONG TITLE**General Description:**

This bill modifies provisions related to the Utah Cyber Center.

Highlighted Provisions:

This bill:

- adds the Department of Environmental Quality as an entity that the Utah Cyber Center will collaborate with when performing legislative duties;
- modifies the deadline for developing a statewide strategic cybersecurity plan;
- expands the Utah Cyber Center's duties to include local education agencies;
- modifies the composition of the Cybersecurity Commission to include a representative from the Utah Education and Telehealth Network;
- creates the Utah Cyber Center Restricted Account; and
- makes technical and conforming changes.

Money Appropriated in this Bill:

None

Other Special Clauses:

None

Utah Code Sections Affected:

AMENDS:

63A-16-1101 (Effective 05/06/26), as enacted by Laws of Utah 2024, Chapter 426

63A-16-1102 (Effective 05/06/26), as last amended by Laws of Utah 2025, First Special Session, Chapter 9

63A-16-1103 (Effective 05/06/26), as renumbered and amended by Laws of Utah 2024, Chapter 426

63C-27-201 (Effective 05/06/26) (Repealed 07/01/32), as enacted by Laws of Utah 2022, Chapter 153

ENACTS:

63A-16-1104 (Effective 05/06/26), Utah Code Annotated 1953

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

Section 1. Section **63A-16-1101** is amended to read:

63A-16-1101 (Effective 05/06/26). Definitions.

As used in this part:

- (1) "Cyber Center" means the Utah Cyber Center created in Section 63A-16-1102.
- (2) "Data breach" means the unauthorized access, acquisition, disclosure, loss of access, or destruction of:
 - (a) personal data affecting 500 or more individuals; or
 - (b) data that compromises the security, confidentiality, availability, or integrity of the computer systems used or information maintained by the governmental entity.
- (3) "Governmental entity" means the same as that term is defined in Section 63G-2-103.
- (4) "Local education agency" means the same as that term is defined in Section 53E-1-102.
- ~~[(4)]~~ (5) "Personal data" means information that is linked or can be reasonably linked to an identified individual or an identifiable individual.

Section 2. Section **63A-16-1102** is amended to read:

63A-16-1102 (Effective 05/06/26). Utah Cyber Center -- Creation -- Duties.

- (1)(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 Cyber Center.
- (2) The division shall operate the 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.
- (3) In addition to the entities described in Subsection ~~[(3)]~~ (2), the 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 53H-4-213.4;
 - (d) the Department of Environmental Quality created in Section 19-1-104;
 - ~~(e)~~ (f) appropriate federal partners, including the Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency;
 - ~~[(e)]~~ (f) appropriate information sharing and analysis centers;

65 [(f)] (g) information technology directors, cybersecurity professionals, or equivalent
66 individuals representing political subdivisions in the state; and
67 [(g)] (h) any other person the division believes is necessary to carry out the duties
68 described in Subsection (4).

69 (4) The Cyber Center shall, within legislative appropriations:

- 70 (a) by ~~[June 30, 2024]~~ January 1, 2027, develop a statewide strategic cybersecurity plan
71 for governmental entities;
72 (b) with respect to executive branch agencies and local education agencies:
73 (i) identify, analyze, and, when appropriate, mitigate cyber threats and vulnerabilities;
74 (ii) coordinate cybersecurity resilience planning;
75 (iii) provide cybersecurity incident response capabilities; and
76 (iv) recommend to the division standards, policies, or procedures to increase the
77 cyber resilience of executive branch agencies individually or collectively;
78 (c) at the request of a governmental entity or local education agency, coordinate
79 cybersecurity incident response for a data breach affecting the governmental entity or
80 local education agency in accordance with Section 63A-19-405;
81 (d) promote cybersecurity standards and best practices for governmental entities and
82 local education agencies;
83 (e) share cyber threat intelligence with governmental entities and, through the Statewide
84 Information and Analysis Center, with other public and private sector organizations;
85 (f) serve as the state cybersecurity incident response repository to receive reports of
86 breaches of system security, including notification or disclosure under Section
87 13-44-202 and data breaches under Section 63A-16-1103;
88 (g) develop incident response plans to coordinate federal, state, local, and private sector
89 activities and manage the risks associated with an attack or malfunction of critical
90 information technology systems within the state;
91 (h) coordinate, develop, and share best practices for cybersecurity resilience in the state;
92 (i) identify sources of funding to make cybersecurity improvements throughout the state;
93 (j) develop a sharing platform to provide resources based on information,
94 recommendations, and best practices; and
95 (k) partner with institutions of higher education and other public and private sector
96 organizations to increase the state's cyber resilience.

97 Section 3. Section **63A-16-1103** is amended to read:

98 **63A-16-1103 (Effective 05/06/26). Assistance to governmental entities and local**

education agencies -- Records.

- (1) The Cyber Center shall provide a governmental entity or local education agency with assistance in responding to a data breach reported under Section 63A-19-405, which may include:
- (a) conducting all or part of an internal investigation into the data breach;
 - (b) assisting law enforcement with the law enforcement investigation if needed;
 - (c) determining the scope of the data breach;
 - (d) assisting the governmental entity in restoring the reasonable integrity of the system;
- or
- (e) providing any other assistance in response to the reported data breach.
- (2)(a) A governmental entity that is required to submit information under Section 63A-19-405 shall provide records to the Cyber Center as a shared record in accordance with Section 63G-2-206.
- (b) The following information may be deemed confidential and may only be shared as provided in Section 63G-2-206:
- (i) the information provided to the Cyber Center by a governmental entity under Section 63A-19-405; and
 - (ii) information produced by the Cyber Center in response to a report of a data breach under Subsection (1).

Section 4. Section **63A-16-1104** is enacted to read:

63A-16-1104 (Effective 05/06/26). Utah Cyber Center Restricted Account -- Creation -- Funding -- Uses.

- (1) There is created within the General Fund a restricted account known as the "Utah Cyber Center Restricted Account."
- (2) The restricted account consists of:
- (a) appropriations made to the account by the Legislature;
 - (b) federal grant funding;
 - (c) private donations, grants, gifts, or bequests; and
 - (d) interest earned on the account.
- (3) The Cyber Center shall administer the account.
- (4) Subject to appropriations, the Cyber Center shall use restricted account money for:
- (a) developing and implementing the statewide strategic cybersecurity plan;
 - (b) providing cybersecurity tools, services, and incident response capabilities to governmental entities and local education agencies;

- (c) conducting cybersecurity assessments and audits for governmental entities and local education agencies;
- (d) providing cybersecurity training and awareness programs;
- (e) acquiring and maintaining cybersecurity technology and infrastructure;
- (f) supporting cyber threat intelligence sharing activities; and
- (g) any other activities necessary to carry out the duties described in Section 63A-16-1102.

(5) The interest earned on account money shall be deposited into the account.

Section 5. Section **63C-27-201** is amended to read:

63C-27-201 (Effective 05/06/26) (Repealed 07/01/32). Cybersecurity Commission created.

(1) There is created the Cybersecurity Commission.

(2) The commission shall be composed ~~[of 24]~~ of the following members:

- (a) one member the governor designates to serve as the governor's designee;
- (b) the commissioner of the Department of Public Safety;
- (c) the lieutenant governor, or an election officer, as that term is defined in Section 20A-1-102, the lieutenant governor designates to serve as the lieutenant governor's designee;
- (d) the chief information officer of the Division of Technology Services;
- (e) the chief information security officer, as described in Section 63A-16-210;
- (f) the chairman of the Public Service Commission shall designate a representative with professional experience in information technology or cybersecurity;
- (g) the executive director of the ~~[Utah]~~ Department of Transportation shall designate a representative with professional experience in information technology or cybersecurity;
- (h) the director of the Division of Finance shall designate a representative with professional experience in information technology or cybersecurity;
- (i) the executive director of the Department of Health and Human Services shall designate a representative with professional experience in information technology or cybersecurity;
- (j) the director of the Division of Indian Affairs shall designate a representative with professional experience in information technology or cybersecurity;
- (k) the Utah League of Cities and Towns shall designate a representative with professional experience in information technology or cybersecurity;

- (l) the Utah Association of Counties shall designate a representative with professional experience in information technology or cybersecurity;
- (m) the attorney general, or the attorney general's designee;
- (n) the commissioner of financial institutions, or the commissioner's designee;
- (o) the executive director of the Department of Environmental Quality shall designate a representative with professional experience in information technology or cybersecurity;
- (p) the executive director of the Department of Natural Resources shall designate a representative with professional experience in information technology or cybersecurity;
- (q) the highest ranking information technology official, or the official's designee, from each of:
- (i) the Judicial Council;
 - (ii) the Utah Board of Higher Education;
 - (iii) the State Board of Education;
 - (iv) the Utah Education and Telehealth Network; and
 - ~~[(iv)]~~ (v) the State Tax Commission;
- (r) the governor shall appoint:
- (i) one representative from the Utah National Guard; and
 - (ii) one representative from the Governor's Office of Economic Opportunity;
- (s) the president of the Senate shall appoint one member of the Senate; and
- (t) the speaker of the House of Representatives shall appoint one member of the House of Representatives.
- (3)(a) The governor's designee shall serve as cochair of the commission.
- (b) The commissioner of the Department of Public Safety shall serve as cochair of the commission.
- (4)(a) The members described in Subsection (2) shall represent urban, rural, and suburban population areas.
- (b) No fewer than half of the members described in Subsection (2) shall have professional experience in cybersecurity or in information technology.
- (5) In addition to the membership described in Subsection (2), the commission shall seek information and advice from state and private entities with expertise in critical infrastructure.
- (6) As necessary to improve information and protect potential vulnerabilities, the

commission shall seek information and advice from federal entities including:

(a) the Cybersecurity and Infrastructure Security Agency;

(b) the Federal Energy Regulatory Commission;

(c) the Federal Bureau of Investigation; and

(d) the United States Department of Transportation.

(7)(a) Except as provided in Subsections (7)(b) and (c), a member is appointed for a term of four years.

(b) A member shall serve until the member's successor is appointed and qualified.

(c) Notwithstanding the requirements of Subsection (7)(a), the governor shall, at the time of appointment or reappointment, adjust the length of terms to ensure that the terms of commission members are staggered so that approximately half of the commission members appointed under Subsection (2)(r) are appointed every two years.

(8)(a) If a vacancy occurs in the membership of the commission, the member shall be replaced in the same manner in which the original appointment was made.

(b) An individual may be appointed to more than one term.

(c) When a vacancy occurs in the membership for any reason, the replacement shall be appointed for the unexpired term.

(9)(a) A majority of the members of the commission is a quorum.

(b) The action of a majority of a quorum constitutes an action of the commission.

(10) The commission shall meet at least two times a year.

Section 6. **Effective Date.**

This bill takes effect on May 6, 2026.