HB0042S02 compared with HB0042

~~{Omitted text}~~ shows text that was in HB0042 but was omitted in HB0042S02
inserted text shows text that was not in HB0042 but was inserted into HB0042S02

DISCLAIMER: This document is provided to assist you in your comparison of the two bills. Sometimes this automated comparison will NOT be completely accurate. Therefore, you need to read the actual bills. This automatically generated document could contain inaccuracies caused by: limitations of the compare program; bad input data; or other causes.

School Cybersecurity Amendments

2026 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Ryan D. Wilcox

Senate Sponsor:

LONG TITLE

General Description:

This bill {~~establishes~~ } directs the State Board of Education to establish minimum cybersecurity standards for local education agencies {~~(LEAs) and expands the Utah Cyber Center's services to include educational institutions~~} .

Highlighted Provisions:

This bill:

- **prohibits certain devices in schools;**
- {~~establishes~~ } directs the Cybersecurity Commission to make rules establishing minimum cybersecurity standards for {~~LEAs~~} local education agencies (LEAs) aligned with industry recognized frameworks;
- {~~**requires LEAs to implement specific cybersecurity measures;**~~}
- {~~**expands the Utah Cyber Center's duties to include services for LEAs;**~~}
- **establishes a phased implementation timeline for LEA compliance;**
- requires coordination {~~between~~ } among the Utah Cyber Center, {~~LEAs~~} the State Board of Education, and the Utah Education and Telehealth Network;

HB0042

- establishes reporting requirements for cybersecurity incidents {~~in educational settings~~} ;
- requires the State Board of Education to {~~develop~~ } provide implementation {~~guidelines~~} support and resources; and
- makes conforming changes.

Money Appropriated in this Bill:

None

Other Special Clauses:

None

Utah Code Sections Affected:

AMENDS:

53G-7-227 (Effective 05/06/26), as last amended by Laws of Utah 2025, First Special Session, Chapter 9

~~**{53H-4-213.4 (Effective 05/06/26), as renumbered and amended by Laws of Utah 2025, First Special Session, Chapter 8}**~~

~~**{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}**~~

~~**{63A-19-101 (Effective 05/06/26), as last amended by Laws of Utah 2025, Chapter 475}**~~

63C-27-201 (Effective 05/06/26) (Repealed 07/01/32), as enacted by Laws of Utah 2022, Chapter 153

63C-27-202 (Effective 05/06/26) (Repealed 07/01/32), as enacted by Laws of Utah 2022, Chapter 153

ENACTS:

53G-8-901 (Effective 05/06/26), Utah Code Annotated 1953

53G-8-902 (Effective 05/06/26), Utah Code Annotated 1953

53G-8-903 (Effective 05/06/26), Utah Code Annotated 1953

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

Section 1. Section **53G-7-227** is amended to read:

53G-7-227. Device prohibition.

(1) As used in this section:

(a)

(i) "AI glasses" means wearable eyewear, whether prescription or non-prescription, that:

(A) incorporates one or more sensors, including cameras, microphones, accelerometers, gyroscopes, or biometric sensors;

(B) uses artificial intelligence, machine learning algorithms, or neural networks to process, analyze, or interpret data captured by the sensors in real-time or near real-time;

(C) provides information, overlays, translations, identification, or other augmented content to the wearer through visual displays, audio output, or haptic feedback; and

(D) may transmit, store, or share data to external devices, networks, or cloud-based services.

(ii) "AI glasses" does not include:

(A) prescription eyeglasses or sunglasses without electronic components;

(B) wearable devices used solely for reading glasses or vision correction without data collection or processing capabilities;

(C) protective eyewear that contains only passive sensors without artificial intelligence processing capabilities; or

(D) virtual reality headsets designed primarily for immersive gaming or entertainment that are not suitable for continuous wear in public settings.

[~~(a)~~] (b) "Cellphone" means a handheld, portable electronic device that is designed to be operated using one or both hands and is capable of transmitting and receiving voice, data, or text communication by means of:

(i) a cellular network;

(ii) a satellite network; or

(iii) any other wireless technology.

[~~(b)~~] (c) "Cellphone" includes:

(i) a smartphone;

(ii) a feature phone;

(iii) a mobile phone;

(iv) a satellite phone; or

(v) a personal digital assistant that incorporates capabilities similar to a smartphone, feature phone, mobile phone, or satellite phone.

[~~(c)~~] (d) "Classroom hours" means:

(i) time during which a student receives scheduled, teacher-supervised instruction that occurs:

(A) in a physical or virtual classroom setting;

(B) during regular school operating hours; and

(C) as part of an approved educational curriculum.

(ii) "Classroom hours" does not include:

(A) lunch periods;

(B) recess;

(C) transit time between classes;

(D) study halls unless directly supervised by a qualified instructor;

(E) after-school activities unless part of an approved extended learning program; or

(F) independent study time occurring outside scheduled instruction.

[~~(d)~~] (e)

(i) "Emerging technology" means any other device that has or will be able to act in place of or as an extension of an individual's cellphone.

(ii) "Emerging technology" does not include school provided or required devices.

[~~(e)~~] (f) "Smart watch" means a wearable computing device that closely resembles a wristwatch or other time-keeping device with the capacity to act in place of or as an extension of an individual's cellphone.

[~~(f)~~] (g) "Smart watch" does not include a wearable device that can only:

(i) tell time;

(ii) monitor an individual's health informatics;

(iii) receive and display notifications or information without the capability to respond; or

(iv) track the individual's physical location.

(2)

(a) An LEA:

(i) shall establish a policy that allows a student to use a cellphone, smart watch, AI glasses, or emerging technology:

(A) to respond to an imminent threat to the health or safety of an individual;

(B) to respond to a school-wide emergency;

(C) to use the SafeUT Crisis Line described in Section 53H-4-210;

(D) for a student's IEP or Section 504 accommodation plan; or

(E) to address a medical necessity; and

(ii) may establish a policy that provides for other circumstances when a student may use a cellphone, smart watch, AI glasses, or emerging technology.

(b) An LEA may establish policies that:

(i) extend restrictions on student use of cellphones, smart watches, or emerging technologies to non-classroom hours during the school day, including:

(A) lunch periods;

(B) transition times between classes; and

(C) other school-supervised activities; and

(ii) impose additional limitations on the use of cellphones, smart watches, or emerging technologies beyond those required by this section.

(3) Except as provided in Subsection (2), a student may not use a cellphone, smart watch, AI glasses, or emerging technology at a school during classroom hours.

(4) The state board may create one or more model policies regarding when a student may use a student's cellphone, smart watch, AI glasses, or emerging technology in a school during classroom hours consistent with this section.

Section 2. Section **2** is enacted to read:

53G-8-901. General provisions -- Definitions.

9. LEA Cybersecurity Standards

As used in this part:

{(1) {~~"CIS Controls" means the Center for Internet Security Critical Security Controls, a prioritized set of actions for cybersecurity that provide specific and actionable ways to defend against common cyber attack methods.}~~ }

(2){(1)} "Cyber Center" means the Utah Cyber Center created in Section 63A-16-1102.

{~~(3) {"Cyber defense plan" means a comprehensive strategy document that outlines an LEA's approach to preventing, detecting, responding to, and recovering from cybersecurity incidents.}~~ }

(4){(2)} "Data breach" means the same as that term is defined in Section 63A-16-1101.

{~~(5) {"Endpoint detection and response" or "EDR" means cybersecurity technology that continuously monitors end-user devices to detect and respond to cyber threats.}~~ }

{~~(6) {"Multi-factor authentication" or "MFA" means an authentication method that requires two or more verification factors to gain access to a resource.}~~ }

{~~(7) {"Patch management" means the process of identifying, acquiring, testing, and installing updates to software and systems to fix vulnerabilities and improve security.}~~ }

{~~(8) {"Personal data" means the same as that term is defined in Section 63A-16-1101.}~~ }

{~~(9) {"Phishing" means a fraudulent attempt to obtain sensitive information by disguising oneself as a trustworthy entity in electronic communications.}~~ }

{~~(10) {"Strong authentication" means enhanced identity verification mechanisms that utilize technologies such as multi-factor authentication, passkeys, or other equivalent or stronger authentication mechanisms that provide comparable or improved levels of security assurance.}~~ }

{~~(11) {"Tabletop exercise" means a discussion-based cybersecurity exercise where team members meet to discuss each team member's roles and responses during an emergency scenario in an informal, low-stress environment.}~~ }

(12){(3)} {~~"Utah~~ } "UETN" means the Utah Education and Telehealth Network{~~" or "UETN" means the network~~ } created in Section 53H-4-213.4.

Section 3. Section **3** is enacted to read:

53G-8-902. {~~Minimum~~ } LEA compliance with cybersecurity standards {~~for an LEA -- Data breach reporting~~ } --State board duties -- Coordination {~~with Utah Cyber Center~~} .

(1) An LEA shall comply with the minimum cybersecurity standards established by the Cybersecurity Commission created in Section 63C-27-201 in rule made in accordance with Subsection 63C-27-202(9).

(2) An LEA shall comply with the minimum cybersecurity standards according to the phased implementation timeline established in rule under Subsection 63C-27-202(9).

(3) The state board, in consultation with the Cyber Center and UETN, shall:

(a) develop implementation guidelines and technical resources to assist LEAs in meeting the minimum cybersecurity standards;

(b) provide technical assistance and support to LEAs;

(1){(c)} {~~Beginning July 1, 2027, each~~ } establish a method to assess LEA {~~shall implement and maintain~~ } compliance with the {~~following~~ } minimum cybersecurity standards{~~:~~} ; and

{~~(a) {implement strong authentication for all staff, administrators, and authorized users accessing LEA systems containing personal data or sensitive information;}~~ }

{~~(b) {designate at least one individual with defined responsibility for overseeing and implementing the LEA's cyber defense plan;}~~ }

{~~(c) {implement endpoint detection and response or equivalent advanced endpoint protection across all LEA-managed devices;}~~ }

(d) {~~provide annual~~ } coordinate the provision of cybersecurity {~~awareness training for all staff, including training on:~~} services and resources to LEAs.

{~~(i) {identifying and reporting phishing attempts;}~~ }

{~~(ii) {strong authentication practices;}~~ }

{~~(iii) {safe data handling procedures; and}~~ }

{~~(iv) {reporting suspicious activity;}~~ }

{~~(e) {establish and maintain regular patch management cycles for all operating systems and applications, with documentation of compliance;}~~ }

{~~(f) {maintain regular, immutable backups with:}~~ }

{~~(i) {redundant storage locations;}~~ }

{~~(ii) {encrypted backup files;}~~ }

(4)

(a) The Cyber Center, the state board, and UETN shall coordinate services to LEAs to:

(iii){(i)} {~~regular testing~~ } avoid duplication of {~~recovery procedures~~} efforts; {~~and~~}

{~~(iv) {documentation of backup and recovery processes;}~~ }

{~~(g) {develop and maintain a documented incident response plan that:}~~ }

(i){(ii)} {~~aligns with~~ } maximize the {~~CIS Controls or equivalent~~ } effectiveness of cybersecurity {~~frameworks~~} resources;

{~~(ii) {includes clear roles and responsibilities;}~~ }

{~~(iii) {establishes communication protocols with the Cyber Center; and}~~ }

{~~(iv) {is tested through regular tabletop exercises at least annually; and}~~ }

{~~(h) {strengthen oversight of third-party vendors by:}~~ }

{~~(i) {maintaining current inventories of all vendors with access to student or staff personal data;}~~ }

{~~(ii) {ensuring all vendor agreements include appropriate data protection clauses;}~~ }

{~~(iii) {conducting regular reviews of vendor security practices; and}~~ }

{~~(iv)~~ {~~ensuring compliance with the state's student data privacy laws.}~~ }

{~~(2)~~ {~~An LEA shall report any data breach to the Cyber Center in accordance with Section 63A-19-405.}~~ }

{~~(3)~~ {~~In addition to the requirements in Section 63A-19-405, an LEA shall:}~~ }

{~~(a)~~ {~~notify the state board within 24 hours of discovering the data breach;}~~ }

{~~(b)~~ {~~coordinate with UETN if the data breach involves network infrastructure or services provided by UETN; and}~~ }

{~~(c)~~ {~~ cooperate with the Cyber Center's investigation and response efforts.}~~ }

{~~(4)~~ {~~The Cyber Center shall provide assistance to an LEA in the same manner the Cyber Center does for any governmental entity as described in Title 63A, Chapter 16, Part 11, Utah Cyber Center.}~~ }

{~~(5)~~ {~~An LEA shall:}~~ }

(iii) ensure LEAs receive consistent guidance and support; and

(a){(iv)} {~~participate in cybersecurity~~ } facilitate information sharing {~~initiatives coordinated by the Cyber Center;~~} regarding cybersecurity threats and best practices.

{~~(b)~~ {~~designate a primary point of contact for cybersecurity matters who shall interface with the Cyber Center and UETN; and}~~ }

(b) The coordination required under Subsection (4)(a) shall include:

(c){(i)} {~~cooperate with statewide~~ } regular meetings among the entities to discuss LEA cybersecurity {~~assessments~~ } needs and {~~improvement~~ } initiatives{~~.~~} ;

(ii) joint development of training materials and resources;

(iii) coordinated response to cybersecurity incidents affecting LEAs; and

(iv) alignment of cybersecurity standards and network infrastructure requirements.

Section 4. Section **4** is enacted to read:

53G-8-903. {~~Coordination between~~ } Data breach reporting -- Coordination with Utah Cyber Center {~~and Utah Education and Telehealth Network~~} .

{~~(1)~~ {~~The Cyber Center and UETN shall coordinate each entity's respective services to an LEA according to the division of responsibilities described in this section.}~~ }

(1) An LEA shall report a data breach to the Cyber Center:

(2){(a)} {~~In~~ } in accordance with Section {~~53H-4-213.4, UETN shall be responsible for network infrastructure and connectivity, including:~~} 63A-19-405; and

{~~(a) {providing and maintaining the physical network infrastructure and Internet connectivity for an LEA;}~~ }

{~~(b) {implementing network-level security controls including firewalls, network segmentation, and traffic monitoring at the infrastructure level;}~~ }

{~~(c) {procuring, installing, and maintaining telecommunication services and equipment on behalf of an LEA;}~~ }

{~~(d) {providing technical support for network connectivity issues;}~~ }

{~~(e) {coordinating with the Cyber Center when network infrastructure is involved in a data breach or security incident; and}~~ }

{~~(f) {implementing network-level security policies that complement the cybersecurity standards required under Section 53G-8-902.}~~ }

{~~(3) {In accordance with Title 63A, Chapter 16, Part 11, Utah Cyber Center, the Cyber Center shall be responsible for a cybersecurity strategy and incident response, including:}~~ }

(a){(b)} {~~developing and maintaining cybersecurity~~ } consistent with standards and {~~best practices for an LEA as required~~ } procedures established in rule under {~~Section 53G-8-902;~~} Subsection 63C-27-202(9).

(2) In addition to the requirements in Section 63A-19-405, an LEA shall:

(b){(a)} {~~providing cybersecurity incident response services when an LEA experiences a~~ } notify the state board within 24 hours of discovering the data breach;

{~~(c) {conducting cybersecurity assessments and vulnerability testing of an LEA's systems;}~~ }

{~~(d) {providing threat intelligence and security alerts to an LEA;}~~ }

{~~(e) {delivering cybersecurity awareness training and resources to an LEA and all relevant staff as the Cyber Center determines;}~~ }

(f){(b)} {~~coordinating~~ } coordinate with UETN {~~when incidents involve~~ } if the data breach involves network infrastructureor services provided by UETN; and

{~~(g) {maintaining the statewide incident response repository for education-related security breaches.}~~ }

(c) cooperate with the Cyber Center's investigation and response efforts.

(3) The Cyber Center shall provide assistance to an LEA in responding to a data breach in the same manner the Cyber Center provides assistance to a governmental entity as described in Title 63A, Chapter 16, Part 11, Utah Cyber Center.

(4) An LEA shall:

{~~(a) {comply with all cybersecurity requirements established in Section 53G-8-902;}~~ }

(a) participate in cybersecurity information sharing initiatives coordinated by the Cyber Center;

(b) designate a primary {~~cybersecurity~~ } point of contact for cybersecurity matters who {~~interfaces~~ } shall interface with {~~both~~ } the Cyber Center {~~for security matters~~ } , the state board, and UETN {~~for network infrastructure matters~~} ;and

{~~(c) {report data breaches to the Cyber Center as required under Section 53G-8-902;}~~ }

{~~(d) {report network infrastructure issues to UETN; and}~~ }

{~~(e) {participate in security initiatives coordinated by both entities within each entity's respective areas of responsibility.}~~ }

{~~(5)~~ }

(c) cooperate with statewide cybersecurity assessments and improvement initiatives.

(5)

(a) A regional education service agency, as that term is defined in Section 53G-4-410, may serve as the designated primary cybersecurity contact for multiple LEAs within the service area.

(b) If a regional education service agency serves as the primary contact under Subsection (5)(a), the agency shall:

(i) coordinate with the Cyber Center , the state board, and UETN on behalf of the participating LEAs;

(ii) ensure each participating LEA meets the {~~requirements of Section 53G-8-902~~} minimum cybersecurity standards established under Subsection 63C-27-202(9); and

(iii) maintain documentation of cybersecurity services provided to each LEA.

{~~(6) {The state board shall: }~~ }

{~~(a) { in consultation with both the Cyber Center and UETN:}~~ }

{~~(i) {develop implementation guidelines that clearly delineate which entity provides specific services; and}~~ }

{~~(ii) {establish a method to assess compliance with this part; and}~~ }

{~~(b) {ensure coordination between the two entities to avoid duplication of services.}~~ }

~~{Section 5. Section **53H-4-213.4** is amended to read: }~~

53H-4-213.4. Educational telecommunications -- Utah Education and Telehealth Network.

(1) There is created the Utah Education and Telehealth Network, or UETN.

(2) UETN shall:

(a) coordinate and support the telecommunications needs of public and higher education, public libraries, and entities affiliated with the state systems of public and higher education as approved by the Utah Education and Telehealth Network Board, including the statewide development and implementation of a network for education, which utilizes satellite, microwave, fiber-optic, broadcast, and other transmission media;

(b) coordinate the various telecommunications technology initiatives of public and higher education;

(c) provide high-quality, cost-effective Internet access and appropriate interface equipment for schools and school systems;

(d) procure, install, and maintain telecommunication services and equipment on behalf of public and higher education;

(e) develop or implement other programs or services for the delivery of distance learning and telehealth services as directed by law;

(f) apply for state and federal funding on behalf of:

(i) public and higher education; and

(ii) telehealth services;

(g) in consultation with health care providers from a variety of health care systems, explore and encourage the development of telehealth services as a means of reducing health care costs and increasing health care quality and access, with emphasis on assisting rural health care providers and special populations; [~~and~~]

(h) in consultation with the Department of Health and Human Services, advise the governor and the Legislature on:

(i) the role of telehealth in the state;

(ii) the policy issues related to telehealth;

(iii) the changing telehealth needs and resources in the state; and

(iv) state budgetary matters related to telehealth[~~.~~] ; and

(i) coordinate with the Utah Cyber Center created in Section 63A-16-1102 to:

(i) implement network-level security controls for local education agencies;

(ii) support cybersecurity incident response when network infrastructure is affected; and

(iii) ensure alignment between network infrastructure and cybersecurity standards required under Section 53G-8-902.

(3) In performing the duties under Subsection (2), UETN shall:

(a) provide services to schools, school districts, and the public and higher education systems through an open and competitive bidding process;

(b) work with the private sector to deliver high-quality, cost-effective services;

(c) avoid duplicating facilities, equipment, or services of private providers or public telecommunications service, as defined under Section 54-8b-2;

(d) utilize statewide economic development criteria in the design and implementation of the educational telecommunications infrastructure; and

(e) assure that public service entities, such as educators, public service providers, and public broadcasters, are provided access to the telecommunications infrastructure developed in the state.

(4) The University of Utah shall provide administrative support for UETN.

(5)

(a) The Utah Education and Telehealth Network Board, which is the governing board for UETN, is created.

(b) The Utah Education and Telehealth Network Board shall have 13 members as follows:

(i) five members representing the state system of higher education, of which at least one member represents technical colleges, appointed by the commissioner of higher education;

(ii) four members representing the state system of public education appointed by the State Board of Education;

(iii) one member representing the state library appointed by the state librarian;

(iv) two members representing hospitals as follows:

(A) the members may not be employed by the same hospital system;

(B) one member shall represent a rural hospital;

(C) one member shall represent an urban hospital; and

(D) the chief administrator or the administrator's designee for each hospital licensed in this state shall select the two hospital representatives; and

(v) one member representing the office of the governor, appointed by the governor.

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

(d)

(i) The Utah Education and Telehealth Network Board shall elect a chair.

(ii) The chair shall set the agenda for the Utah Education and Telehealth Network Board meetings.

(6) A member of the Utah Education and Telehealth Network Board may not receive compensation or benefits for the member's service, but may receive per diem and travel expenses in accordance with:

(a) Section 63A-3-106;

(b) Section 63A-3-107; and

(c) rules made by the Division of Finance pursuant to Sections 63A-3-106 and 63A-3-107.

(7) The Utah Education and Telehealth Network Board:

(a) shall hire an executive director for UETN who may hire staff for UETN as permitted by the budget;

(b) may terminate the executive director's employment or assignment;

(c) shall determine the executive director's salary;

(d) shall annually conduct a performance evaluation of the executive director;

(e) shall establish policies the Utah Education and Telehealth Network Board determines are necessary for the operation of UETN and the administration of UETN's duties; and

(f) shall advise UETN in:

(i) the development and operation of a coordinated, statewide, multi-option telecommunications system to assist in the delivery of educational services and telehealth services throughout the state; and

(ii) acquiring, producing, and distributing instructional content.

(8) The executive director of UETN shall be an at-will employee.

(9) UETN shall locate and maintain educational and telehealth telecommunication infrastructure throughout the state.

(10) Educational institutions shall manage site operations under policy established by UETN.

(11) Subject to future budget constraints, the Legislature shall provide an annual appropriation to operate UETN.

(12) If the network operated by the Division of Technology Services is not available, UETN may provide network connections to the central administration of counties and municipalities for the sole purpose of transferring data to a secure facility for backup and disaster recovery.

~~{Section 6. Section **63A-16-1101** is amended to read: }~~

63A-16-1101. 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 and includes a local education agency as that term is defined in Section 53E-1-102.

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

(5) "Utah Education and Telehealth Network" or "UETN" means the network created in Section 53H-4-213.4.

~~{Section 7. Section **63A-16-1102** is amended to read: }~~

63A-16-1102. 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) appropriate federal partners, including the Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency;

(e) appropriate information sharing and analysis centers;

(f) information technology directors, cybersecurity professionals, or equivalent individuals representing political subdivisions and local education agencies, as that term is defined in Section 53E-1-102, in the state; and

(g) any other person the division believes is necessary to carry out the duties described in Subsection (4).

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

(a) [~~by June 30, 2024,~~]develop a statewide strategic cybersecurity plan for 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 a data breach affecting the governmental entity in accordance with Section 63A-19-405;

(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 repository to receive reports of breaches of system security, including notification or disclosure under Section 13-44-202 and data breaches under Section 63A-16-1103;

(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, the Utah Education and Telehealth Network, and other public and private sector organizations to increase the state's cyber resilience[~~.~~] ; and

(l) provide cybersecurity services to a local education agency as defined in Section 53E-1-102, including:

(i) cybersecurity assessments and vulnerability testing;

(ii) incident response coordination and support;

(iii) threat intelligence sharing relevant to the education sector;

(iv) technical assistance in implementing cybersecurity standards required under Section 53G-8-902;

(v) cybersecurity awareness training resources; and

(vi) coordination with the Utah Education and Telehealth Network on relevant security matters in accordance with Section 53H-4-213.4.

~~{Section 8. Section **63A-16-1103** is amended to read: }~~

63A-16-1103. Assistance to governmental entities -- Records.

(1) The Cyber Center shall provide a governmental entity 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) the information produced by the Cyber Center in response to a report of a data breach under Subsection (1).

(3) In addition to all requirements for a governmental entity in this part, a local education agency shall submit information in accordance with Section 53G-8-902.

~~{Section 9. Section **63A-19-101** is amended to read: }~~

63A-19-101. Definitions.

As used in this chapter:

(1) "Anonymized data" means information that has been irreversibly modified so that there is no possibility of using the information, alone or in combination with other information, to identify an individual.

(2) "At-risk government employee" means the same as that term is defined in Section 63G-2-303.

(3) "Automated decision making" means using personal data to make a decision about an individual through automated processing, without human review or intervention.

(4) "Biometric data" means the same as that term is defined in Section 13-61-101.

(5) "Chief administrative officer" means the same as that term is defined in Section 63A-12-100.5.

(6) "Chief privacy officer" means the individual appointed under Section 63A-19-302.

(7) "Commission" means the Utah Privacy Commission established in Section 63A-19-203.

(8) "Contract" means an agreement between a governmental entity and a person for goods or services that involve personal data.

(9)

(a) "Contractor" means a person who:

(i) has entered into a contract with a governmental entity; and

(ii) may process personal data under the contract.

(b) "Contractor" includes a contractor's employees, agents, or subcontractors.

(10) "Cyber Center" means the Utah Cyber Center created in Section 63A-16-1102.

(11) "Data breach" means the unauthorized access, acquisition, disclosure, loss of access, or destruction of personal data held by a governmental entity, unless the governmental entity concludes, according to standards established by the Cyber Center, that there is a low probability that personal data has been compromised.

(12) "De-identified data" means information from which personal data has been removed or obscured so that the information is not readily identifiable to a specific individual, and which may not be re-identified.

(13) "Genetic data" means the same as that term is defined in Section 13-60-102.

(14) "Governing board" means the Utah Privacy Governing Board established in Section 63A-19-201.

(15) "Governmental entity" means the same as that term is defined in Section 63G-2-103 and includes a local education agency as that term is defined in Section 53E-1-102.

(16) "Government website" means a set of related web pages that is operated by or on behalf of a governmental entity and is:

(a) located under a single domain name or web address; and

(b) accessible directly through the Internet or by the use of a software program.

(17)

(a) "High-risk processing activities" means a governmental entity's processing of personal data that may have a significant impact on an individual's privacy interests, based on factors that include:

(i) the sensitivity of the personal data processed;

(ii) the amount of personal data being processed;

(iii) the individual's ability to consent to the processing of personal data; and

(iv) risks of unauthorized access or use.

(b) "High-risk processing activities" may include the use of:

(i) facial recognition technology;

(ii) automated decision making;

(iii) profiling;

(iv) genetic data;

(v) biometric data; or

(vi) geolocation data.

(18) "Independent entity" means the same as that term is defined in Section 63E-1-102.

(19) "Individual" means the same as that term is defined in Section 63G-2-103.

(20) "Legal guardian" means:

(a) the parent of a minor; or

(b) an individual appointed by a court to be the guardian of a minor or incapacitated individual and given legal authority to make decisions regarding the person or property of the minor or incapacitated individual.

(21) "Office" means the Utah Office of Data Privacy created in Section 63A-19-301.

(22) "Ombudsperson" means the data privacy ombudsperson appointed under Section 63A-19-501.

(23) "Person" means the same as that term is defined in Section 63G-2-103.

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

(25) "Privacy annotation" means a summary of personal data contained in a record series as described in Section 63A-19-401.1.

(26) "Privacy practice" means a governmental entity's:

(a) organizational, technical, administrative, and physical safeguards designed to protect an individual's personal data;

(b) policies and procedures related to the acquisition, use, storage, sharing, retention, and disposal of personal data; and

(c) practice of providing notice to an individual regarding the individual's privacy rights.

(27) "Process," "processing," or "processing activity" means any operation or set of operations performed on personal data, including collection, recording, organization, structuring, storage, adaptation, alteration, access, retrieval, consultation, use, disclosure by transmission, transfer, dissemination, alignment, combination, restriction, erasure, or destruction.

(28) "Profiling" means the processing of personal data to evaluate or predict an individual's:

(a) economic situation;

(b) health;

(c) personal preferences;

(d) interests;

(e) reliability;

(f) behavior;

(g) location; or

(h) movements.

(29) "Purchase" or "purchasing" means the exchange of monetary consideration to obtain the personal data of an individual who is not a party to the transaction.

(30) "Record" means the same as that term is defined in Section 63G-2-103.

(31) "Record series" means the same as that term is defined in Section 63G-2-103.

(32) "Retention schedule" means a governmental entity's schedule for the retention or disposal of records that has been approved by the Records Management Committee pursuant to Section 63A-12-113.

(33)

(a) "Sell" means an exchange of personal data for monetary consideration by a governmental entity to a third party.

(b) "Sell" does not include a fee:

(i) charged by a governmental entity for access to a record pursuant to Section 63G-2-203; or

(ii) assessed in accordance with an approved fee schedule.

(34)

(a) "State agency" means the following entities that are under the direct supervision and control of the governor or the lieutenant governor:

(i) a department;

(ii) a commission;

(iii) a board;

(iv) a council;

(v) an institution;

(vi) an officer;

(vii) a corporation;

(viii) a fund;

(ix) a division;

(x) an office;

(xi) a committee;

(xii) an authority;

(xiii) a laboratory;

(xiv) a library;

(xv) a bureau;

(xvi) a panel;

(xvii) another administrative unit of the state; or

(xviii) an agent of an entity described in Subsections (34)(a)(i) through (xvii).

(b) "State agency" does not include:

(i) the legislative branch;

(ii) the judicial branch;

(iii) an executive branch agency within the Office of the Attorney General, the state auditor, the state treasurer, or the State Board of Education; or

(iv) an independent entity.

(35) "State privacy auditor" means the same as that term is defined in Section 67-3-13.

(36) "Synthetic data" means artificial data that:

(a) is generated from personal data; and

(b) models the statistical properties of the original personal data.

(37) "User" means an individual who accesses a government website.

(38)

(a) "User data" means any information about a user that is automatically collected by a government website when a user accesses the government website.

(b) "User data" includes information that identifies:

(i) a user as having requested or obtained specific materials or services from a government website;

(ii) Internet sites visited by a user;

(iii) the contents of a user's data-storage device;

(iv) any identifying code linked to a user of a government website; and

(v) a user's:

(A) IP or Mac address; or

(B) session ID.

(39) "Website tracking technology" means any tool used by a government website to:

(a) monitor a user's behavior; or

(b) collect user data.

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

63C-27-201. Cybersecurity Commission created.

(1) There is created the Cybersecurity Commission.

(2) The commission shall be composed of [~~24~~] 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 state superintendent of public instruction or the state superintendent's designee;)~~ }

(r)(q) two local education agency employees tasked with job duties that include systems and security management from one charter school and one school district whom the state superintendent selects;

[~~(q)~~] (s){(r)} 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; and

(iv) the State Tax Commission;

[~~(r)~~] (t){(s)} 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)~~] (u){(t)} the president of the Senate shall appoint one member of the Senate; and

[~~(t)~~] (v){(u)} 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)~~] (2) 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. Section **63C-27-202** is amended to read:

63C-27-202. Commission duties.

The commission shall:

(1) identify and inform the governor of:

(a) cyber threats and vulnerabilities towards Utah's critical infrastructure;

(b) cybersecurity assets and resources; and

(c) an analysis of:

(i) current cyber incident response capabilities;

(ii) potential cyber threats; and

(iii) areas of significant concern with respect to:

(A) vulnerability to cyber attack; or

(B) seriousness of consequences in the event of a cyber attack;

(2) provide resources with respect to cyber attacks in both the public and private sector, including:

(a) best practices;

(b) education; and

(c) mitigation;

(3) promote cyber security awareness;

(4) share information;

(5) promote best practices to prevent and mitigate cyber attacks;

(6) enhance cyber capabilities and response for all Utahns;

(7) provide consistent outreach and collaboration with private and public sector organizations;[~~and~~]

(8) share cyber threat intelligence to operators and overseers of Utah's critical infrastructure[~~.~~] ; and

(9) in accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act, make rules establishing minimum cybersecurity standards for a local education agency, as that term is defined in Section 53G-3-402, that:

(a) align with industry recognized cybersecurity frameworks and standards, including frameworks developed by the National Institute of Standards and Technology, the Center for Internet Security, or a successor organization;

(b) take into account varying local education agency resources, capacity, and needs;

(c) establish phased implementation timelines based on local education agency size, existing cybersecurity infrastructure, and available resources; and

(d) as appropriate based on the local education agency's size, risk profile, and available resources, shall address:

(i) identity and access management;

(ii) asset management and inventory of hardware, software, and data systems;

(iii) data protection;

(iv) security monitoring and logging capabilities;

(v) vulnerability management, including regular security assessments and patching procedures;

(vi) incident response and recovery planning;

(vii) security awareness training requirements for staff and administrators;

(viii) third-party risk management for vendors with access to local education agency systems or data;

(ix) network security controls;

(x) backup and disaster recovery procedures; and

(xi) governance structures for cybersecurity oversight within a local education agency.

Section 7. **Effective date.**

Effective Date.

This bill takes effect on May 6, 2026.

2-4-26 11:17 AM