Ryan D. Wilcox proposes the following substitute bill:

School Cybersecurity Amendments

2026 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Ryan D. Wilcox

Senate Sponsor:

LONG TITLE

General Description:

This bill directs the State Board of Education to establish minimum cybersecurity standards for local education agencies.

Highlighted Provisions:

This bill:

- prohibits certain devices in schools;
- directs the Cybersecurity Commission to make rules establishing minimum cybersecurity standards for local education agencies (LEAs) aligned with industry recognized frameworks;
- establishes a phased implementation timeline for LEA compliance;
- requires coordination among the Utah Cyber Center, the State Board of Education, and the Utah Education and Telehealth Network;
- establishes reporting requirements for cybersecurity incidents;
- requires the State Board of Education to provide implementation 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

63C-27-201 (Effective 05/06/26) (Repealed 07/01/32), as enacted by Laws of Utah 2022,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63C-27-202 (Effective 05/06/26) (Repealed 07/01/32), as enacted by Laws of Utah 2022, Chapter 153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 (Effective 05/06/26). 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 **53G-8-901** is enacted to read:

Part 9. LEA Cybersecurity Standards

53G-8-901 (Effective 05/06/26). General provisions -- 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 same as that term is defined in Section 63A-16-1101.

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

Section 3. Section **53G-8-902** is enacted to read:

53G-8-902 (Effective 05/06/26). LEA compliance with cybersecurity standards --State board duties -- Coordination.

(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;

(c) establish a method to assess LEA compliance with the minimum cybersecurity standards; and

(d) coordinate the provision of cybersecurity services and resources to LEAs.

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

(i) avoid duplication of efforts;

(ii) maximize the effectiveness of cybersecurity resources;

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

(iv) facilitate information sharing regarding cybersecurity threats and best practices.

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

(i) regular meetings among the entities to discuss LEA cybersecurity needs and 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 **53G-8-903** is enacted to read:

53G-8-903 (Effective 05/06/26). Data breach reporting -- Coordination with Utah Cyber Center.

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

(a) in accordance with Section 63A-19-405; and

(b) consistent with standards and procedures established in rule under Subsection 63C-27-202(9).

(2) 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.

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

(b) designate a primary point of contact for cybersecurity matters who shall interface with the Cyber Center, the state board, and UETN; and

(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 minimum cybersecurity standards established under Subsection 63C-27-202(9); and

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

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~~] 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) 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)~~] (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)~~] (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)~~] (t) the president of the Senate shall appoint one member of the Senate; and

[~~(t)~~] (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 (Effective 05/06/26) (Repealed 07/01/32). 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.**

This bill takes effect on May 6, 2026.