THIRD READING

Bill No: AB 2298
Author: Irwin (D)
Amended: 8/20/26 in Senate
Vote: 21

SENATE EDUCATION COMMITTEE: 7-0, 6/17/26
AYES: Pérez, Ochoa Bogh, Cabaldon, Choi, Cortese, Gonzalez, Reyes

SENATE APPROPRIATIONS COMMITTEE: Senate Rule 28.8

ASSEMBLY FLOOR: 68-0, 5/21/26 (Consent) - See last page for vote

SUBJECT: Pupil instruction: computer science: content standards and instructional materials

SOURCE: Author

DIGEST: This bill requires the Instructional Quality Commission (IQC), during the next revision of the computer science content standards occurring after January 1, 2027, to consider incorporating cybersecurity skills content into those standards.

Senate floor amendments of 8/20/26 strike a provision of this bill requiring the IQC to consider including cybersecurity skills in its criteria for evaluating instructional materials, when such materials are next adopted by the State Board of Education (SBE).

ANALYSIS:

Existing law:

1) Requires, on or before July 31, 2019, the IQC to consider developing and recommending to the SBE computer science content standards for kindergarten (K) and grades 1 to 12, inclusive, as specified. States that the computer science content standards may be used by school districts to develop computer science

programs and course assessments but are not mandatory. (Education Code (EC) § 60605.4)

2) Requires the SBE to adopt at least five instructional materials for grades K-8 in the following subjects:

   a) Language arts;

   b) Mathematics;

   c) Science;

   d) Social science;

   e) Bilingual or bicultural subjects; and

   f) Any other subject, discipline, or interdisciplinary areas for which the SBE determines the adoption of instructional materials to be necessary or desirable. (EC § 60200)

3) Establishes procedures for the adoption of instructional materials for grades K-8 by the SBE. (EC § 60200)

4) Authorizes a process for conducting a follow-up adoption of instructional materials, and defines it as one other than the primary adoption. (EC § 60227)

5) Authorizes local educational agencies (LEAs) to use instructional materials that are aligned with state adopted academic content standards, including instructional materials that have not been adopted by the SBE. (EC § 60210)

6) Requires that if an LEA chooses to use instructional materials that have not been adopted by the SBE, the LEA shall ensure that a majority of the participants of any review process it conducts are classroom teachers who are assigned to the subject area or grade level of the materials. (EC § 60210)

This bill:

1) Requires the IQC to consider incorporating cybersecurity skills content during the next revision of the computer science content standards occurring after January 1, 2027.

2) Defines "cybersecurity skills" to mean techniques to protect information and devices by preventing, detecting, and responding to attacks by threat actors.

Comments

Need for the bill. According to the author, "Recent years have seen a stark increase in the number and sophistication of cyber threats posed to the students in our state, underscoring the need for modernized cybersecurity education. Existing computer science content standards, last updated in 2018, include cybersecurity content, but they focus primarily on protecting information rather than identifying and preventing threats. While this foundation has value, it reflects an outdated generation of cyber risks."

"Since 2018, cyberattacks have grown increasingly complex, particularly with the growth of artificial intelligence, enabling more advanced phishing schemes, social engineering, and automated attacks. As a result, our existing standards no longer align with the current cyber threat landscape. Modern cybersecurity education standards must emphasize the skills needed to identify, prevent, and respond to these increasingly sophisticated attacks."

"AB 2298 addresses this gap by requiring the Instructional Quality Commission to consider including updated, more robust cybersecurity skills content focused on identifying and responding to threats into the state's computer science standards. This will ensure that, as cyber threats continue to evolve, students are equipped with the knowledge and skills needed to protect themselves and respond effectively to the modern cyber threats they face today."

Computer Science Standards for California Public Schools: Kindergarten through Grade Twelve. In September 2018, the SBE adopted the California Computer Science Standards based on the revised International Computer Science Teachers Association standards, which align with the national K–12 Computer Science Framework.

The standards include five core concept areas which are each coupled with seven core practices. Each core concept provides foundational knowledge on key ideas, which build upon each other as students progress through grade spans. Core practices help demonstrate ways in which students actively engage in computer science learning experiences that build conceptual knowledge.

Cybersecurity in the Computer Science Standards. This bill requires the IQC, during its next revision of the Computer Science Standards, to consider incorporating content on cybersecurity skills. Currently, cybersecurity content is featured across all grade spans in the Computer Science Standards as a subconcept under the Networks and the Internet (NI) core concept. Examples within the standards include, but are not limited to, the following:

Kindergarten through Grade 2

Standard: K-2.NI.5 - Explain why people use passwords.

Descriptive Statement: Passwords protect information from unwanted use by others. When creating passwords, people often use patterns of familiar numbers and text to more easily remember their passwords. However, this may make the passwords weaker. Knowledge about the importance of passwords is an essential first step in learning about cybersecurity. Students explain that strong passwords are needed to protect devices and information from unwanted use. For example, students could play a game of guessing a three-character code. In one version of the game, the characters are only numbers. In the second version, characters are numbers or letters. Students describe why it would take longer to guess the correct code in the second case. Alternatively, students could engage in a collaborative discussion regarding passwords and their importance. Students may follow up the discussion by exploring strong password components (combination of letters, numbers, and characters), creating their own passwords, and writing opinion pieces indicating reasons their passwords are strong.

Grades 3 through 5

Standard: 3-5.NI.5 - Describe physical and digital security measures for protecting personal information.

Descriptive Statement: Personal information can be protected physically and digitally. Cybersecurity is the protection from unauthorized use of electronic data, or the measures taken to achieve this. Students identify what personal information is and the reasons for protecting it. Students describe physical and digital approaches for protecting personal information, such as using strong passwords and biometric scanners. For example, students could engage in a collaborative discussion orally or in writing regarding topics that relate to personal cybersecurity issues. Discussion topics could be based on current events related to cybersecurity or topics that are applicable to students, such as the necessity of backing up data to guard against loss, how to create strong passwords, and the importance of not sharing passwords, or why we should keep operating systems updated and use anti-virus software to protect data and systems. Students could also discuss physical measures that can be used to protect data, including biometric scanners, locked doors, and physical backups.

Grades 9 through 12

Standard: 9-12.NI.6 - Compare and contrast security measures to address various security threats.

Descriptive Statement: Network security depends on a combination of hardware, software, and practices that control access to data and systems. The needs of users and the sensitivity of data determine the level of security implemented. Potential security problems, such as denial-of-service attacks, ransomware, viruses, worms, spyware, and phishing, present threats to sensitive data. Students compare and contrast different types of security measures based on factors such as efficiency, feasibility, ethical impacts, usability, and security. For example, students could review case studies or current events in which governments or organizations experienced data leaks or data loss as a result of these types of attacks. Students could provide an analysis of actual security measures taken compared to other security measures which may have led to different outcomes. Alternatively, students might discuss computer security policies in place at the local level that present a tradeoff between usability and security, such as a web filter that prevents access to many educational sites but keeps the campus network safe.

The IQC and the SBE. The Legislature has vested the IQC and the SBE with the authority to develop and adopt state content standards, curriculum frameworks, and instructional materials. The content standards describe the knowledge, concepts, and skills that educators and professionals in the field expect students to know at each grade level. Curriculum frameworks provide guidance for implementing the content standards by describing the scope and sequence of knowledge and the skills that all students are expected to master.

The IQC develops curriculum frameworks through a process involving practitioners and experts who have an in-depth understanding of curriculum and instruction, including the full scope and sequence of the curriculum in each subject and at each grade level, constraints on instructional time and resources, and the relationship of curriculum to state assessments and other measures of student progress. Changes are frequently made in response to public comment. The frameworks are then adopted by the SBE in a public meeting.

The resulting curriculum framework is intended to serve as a guidance document for educators and administrators on how to plan for and provide quality, skills-based, standards-aligned instruction on the various content areas.

FISCAL EFFECT: Appropriation: No Fiscal Com.: Yes Local: No

SUPPORT: (Verified 8/19/26)

Alameda County Office of Education
Business Software Alliance
California Chamber of Commerce
California State PTA
California Teachers Association
Computer & Communications Industry Association
Electronic Frontier Foundation
Mastercard
OpenAI
Silicon Valley Leadership Group
Software & Information Industry Association
TechNet

OPPOSITION: (Verified 8/19/26)

None received

ASSEMBLY FLOOR: 68-0, 5/21/26
AYES: Addis, Aguiar-Curry, Ahrens, Alanis, Alvarez, Ávila Farías, Bains, Bauer-Kahan, Bennett, Berman, Boerner, Bonta, Bryan, Calderon, Caloza, Carrillo, Castillo, Connolly, Davies, DeMaio, Dixon, Elhawary, Ellis, Flora, Fong, Gallagher, Gipson, Jeff Gonzalez, Mark González, Hadwick, Haney, Harabedian, Hart, Irwin, Jackson, Johnson, Kalra, Krell, Lee, Macedo, McKinnor, Muratsuchi, Nguyen, Ortega, Pacheco, Papan, Patel, Patterson, Pellerin, Petrie-Norris, Quirk-Silva, Ransom, Michelle Rodriguez, Rogers, Blanca Rubio, Sanchez, Schiavo, Sharp-Collins, Solache, Soria, Stefani, Ta, Tangipa, Valencia, Wallis, Ward, Zbur, Rivas
NO VOTE RECORDED: Arambula, Chen, Gabriel, Garcia, Hoover, Lackey, Lowenthal, Ramos, Celeste Rodriguez, Schultz, Wicks, Wilson

Prepared by: Therresa Austin / ED. / (916) 651-4105
8/24/26 13:43:42

****** END ******