SENATE COMMITTEE ON EDUCATION
Senator Sasha Renée Pérez, Chair
2025 - 2026 Regular

Bill No:	AB 2298	**Hearing Date:**	June 17, 2026
Author:	Irwin		
Version:	March 19, 2026		
Urgency:	No	**Fiscal:**	Yes
Consultant:	Therresa Austin		

Subject: Pupil instruction: computer science: content standards and instructional materials.

SUMMARY

This bill requires the Instructional Quality Commission (IQC) to consider incorporating content on cybersecurity skills during its next revision of the Computer Science Content Standards and the evaluation criteria for adopted instructional materials in computer science after January 1, 2027.

BACKGROUND

Existing law:

1) Requires, on or before July 31, 2019, the IQC to consider developing and recommending to the State Board of Education (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)

ANALYSIS

This bill:

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

2) Requires the IQC, during the next SBE adoption of instructional materials adoption occurring after January 1, 2027, to consider including cybersecurity skills in its criteria for evaluating instructional materials.

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

STAFF COMMENTS

1) ***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."

2) ***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. The computer science core concepts include:

a) Computing Systems

b) Networks and the Internet

c) Data and Analysis

d) Algorithms and Programming

e) Impacts of Computing

The computer science core practices include:

a) Fostering an Inclusive Computing Culture

b) Collaborating Around Computing

c) Recognizing and Defining Computational Problems

d) Developing and Using Abstractions

e) Creating Computational Artifacts

f) Testing and Refining Computational Artifacts

g) Communicating About Computing

3) ***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.

4) ***Computer Science Strategic Implementation Plan (CSSIP)***. In 2016, the Legislature passed AB 2329 (Bonilla, Chapter 693, Statutes of 2016), requiring the SBE to create the CSSIP that addresses the following topics:

a) Broadening the pool of teachers to teach computer science.

b) Defining computer science education principles that meet the needs of pupils in kindergarten and grades one to twelve, inclusive.

c) Ensuring that all pupils have access to quality computer science courses.

The development of the CSSIP was a multi-step process that involved 23 panel members, comprising teachers, administrators, faculty from institutions of higher education (IHEs), a public school student, representatives from private industry, a parent organization, the California Commission on Teacher Credentialing (CTC), and the IQC. Members were selected based on their expertise and leadership in computer science education, experience in standards-based interdisciplinary and differentiated instruction for diverse student populations, and previous committee experience.

The final CSSIP includes activities and recommendations organized into three sections: Equity and Access, Supporting Educators to Teach Computer Science, and Expanding Computer Science Course Offerings. Each section provides the following:

a) A brief overview of the topic, its current status, and why it is important;

b) A description of state activities, both those that the state plans to implement right away and those that should be considered pending funding; and

c) Expert suggestions and guidance for schools, districts, county offices of education (COEs), community and business partners, and other entities to consider as they work to improve computer science education for the students in their local schools and communities.

5) ***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 a 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.

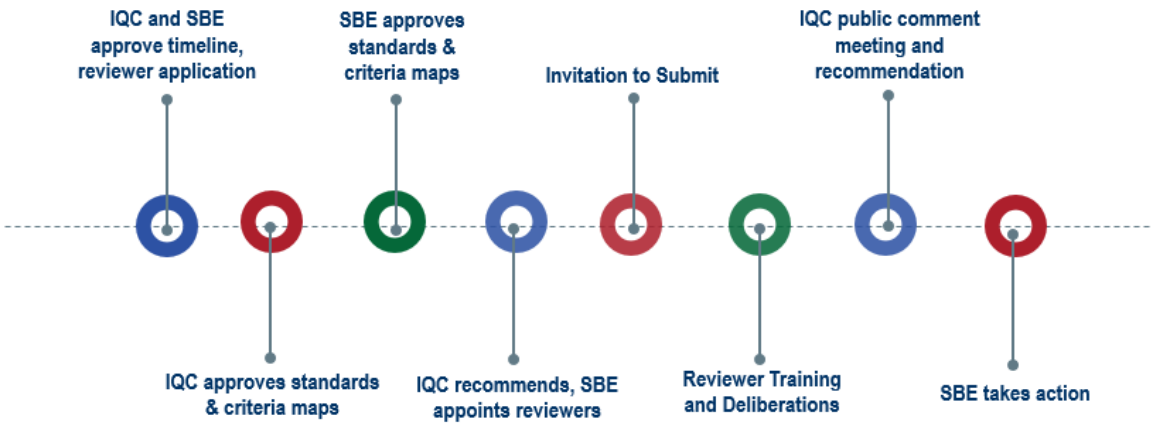
The resulting curriculum framework is intended to serve as a guidance document for educators and administrators on how to plan for and provide quality, skills-based, standards-aligned instruction on the various content areas.

6) ***Instructional Materials Adoption Process.*** State law requires the IQC to recommend and the SBE to adopt instructional materials for grades K-8 in the curriculum areas of English language arts/English language development, mathematics, science, history–social science, visual and performing arts, health, and world languages.

Each new instructional materials adoption process is typically initiated after adopting a new or revised curriculum framework—each of which contains a chapter describing the criteria for evaluation of instructional materials.

According to CDE, the instructional materials adoption process (summarized in the sample timeline below) takes place over a period of approximately two years.

Sample Instructional Materials Adoption Timeline with Key Milestones



CA Department of Education, Nov 2023

Once adopted by the SBE, school district governing boards and charter schools may adopt the instructional materials or separately adopt materials that have not been adopted by the SBE but have been reviewed to be in alignment with the state SBE adopted content standards and curricular frameworks.

This bill requires the IQC, the next time the instructional materials in computer science are adopted by SBE after January 1, 2027, to consider including cybersecurity skills in its criteria for evaluating instructional materials. Notably, while the SBE adopted inaugural computer science content standards in 2018, it has never adopted instructional materials for computer science in the years that followed. Instead, the CDE maintains a computer science resource page that lists classroom-based resources to support computer science instruction that are based on recommendations from the Computer Science Strategic Implementation Plan Panel.

7) ***The Curriculum Guidance Study and future of curriculum development and adoption.*** The 2025-26 budget, through AB 121 (Committee on Budget, Chapter 8, Statutes of 2025), included $1 million for a Curriculum Guidance Study to evaluate the processes by which other states develop curriculum guidance, and to make recommendations about how to improve and streamline California's processes across all content areas. The report is required to include, among other topics:

   a) The roles and responsibilities of the CDE, the IQC, the SBE, the Legislature, LEAs, educators, parents and guardians, and the public; and

   b) The processes and cycles for developing, revising, and adopting content standards, curriculum frameworks, and other instructional guidance, and how available instructional time in elementary and secondary schools is considered.

   This report is to be completed by January 1, 2027.

8) ***Prior and related legislation.***

   AB 2097 (Berman, 2024) would have established a voluntary California Computer Science Demonstration Project and a corresponding California Computer Science Demonstration Project Working Group for the purposes of expanding computer science course access to eligible public high schools and collect data on computer science course enrollment. *AB 2097 was held in the Senate Appropriations Committee.*

   AB 1054 (Berman, 2023) would have required LEAs and charter schools maintaining any of grades 9 to 12 to adopt a plan to offer at least one course in computer science education beginning in the 2025-26 school year, as specified. *AB 1054 was held in the Senate Appropriations Committee.*

   AB 1251 (Luz Rivas, Chapter 834, Statutes of 2023) establishes a workgroup to determine which single subject credentials should authorize the teaching of computer science, and to report recommendations to the Legislature.

AB 130 (Committee on Budget, Chapter 44, Statutes of 2021) established the Computer Science Supplementary Authorization Incentive Grant Program for the purpose of providing one-time grants to LEAs to support the preparation of credentialed teachers to earn a supplementary authorization in computer science and provide instruction in computer science coursework.

AB 128 (Ting, Chapter 21, Statutes of 2021) appropriated $5 million on a one-time basis to establish the Educator Workforce Investment Grant: Computer Science, and required the CDE to select an institution of higher education or nonprofit organizations to provide professional learning for teachers and paraprofessionals statewide in strategies for providing high-quality instruction and computer science learning experiences aligned to the computer science content standards.

AB 2274 (Berman, 2020) would have required the CDE to annually compile and post on its website a report on computer science courses, course enrollment, and teachers of computer science courses, for the 2019-20 school year and each subsequent school year. *AB 2274 was held in the Assembly Education Committee.*

AB 20 (Berman, 2020) would have established a Computer Science Coordinator position at the CDE. *AB 20 was held in the Assembly Appropriations Committee.*

AB 52 (Berman, 2019) would have required the CSSIP to be regularly updated. *AB 52 was held in the Assembly Appropriations Committee.*

AB 2329 (Bonilla, Chapter 693, Statutes of 2016) requires the SPI to convene a computer science strategic implementation advisory panel to develop recommendations for the CSSIP.

SUPPORT

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

OPPOSITION

None received

-- END --