

COMMITTEE LEADERSHIP

Erin Hannigan, District 1
Monica Brown, District 2

STAFF

Matthew A. Davis, CAO



**Legislative
Committee**

**Monday, March 4, 2024
1:30 p.m. – 3 p.m.**

Solano County Administration Center
675 Texas Street, Conf. Rm 6003 (6th Floor), Fairfield, CA 94533
Call in option on MS Teams: (323) 457-3408, ID 590 649 492#

MEETING AGENDA

(1) – INTRODUCTIONS *(Attendees)*

Erin Hannigan, District 1 Supervisor and Monica Brown, District 2 Supervisor

(2) – SELECTION OF THE LEGISLATIVE COMMITTEE CHAIR *(Action Item)*

(2) – ADDITIONS / DELETIONS TO THE AGENDA

(3) – PUBLIC COMMENT *(Items not on the agenda)*

(4) – FEDERAL LEGISLATIVE UPDATE

Paragon Government Relations, Washington D.C.

- (1) Fiscal Year 2024 Appropriations Update
- (2) Fiscal Year 2025 Budget Outlook
 - a. Fiscal Year 2025 Earmark Process
- (3) Rep. Garamendi introduces HOME Investment Partnerships Reauthorization and Improvement Act
- (4) Housing for All Act Press Conference
- (5) Update on Affordable Connectivity Program

(5) – UPDATE FROM SOLANO COUNTY LEGISLATIVE DELEGATION

Representative and/or staff

(6) – STATE LEGISLATIVE UPDATE

Karen Lange, SYASL Partners, Inc., Sacramento, CA

- (1) State Budget update
- (2) Sponsor [AB 1957](#) Best Value legislation
- (3) Receive an update on [AB 749](#), state agencies, information security, uniform standards
- (4) Receive an update on [SB 1047](#), safe and secure innovation for frontier artificial intelligence systems act

>> Continued next page

COMMITTEE LEADERSHIP

Erin Hannigan, District 1
Monica Brown, District 2



Legislative Committee

STAFF

Matthew A. Davis, CAO

(7) – ACTION ITEMS

- (1) Receive an update on [AB 1957](#), ([Wilson – D](#)) an Act to amend sections of the Public Contract Code, relating to public contracts, and consider making a recommendation (*Recommended by General Services, presented by Karen Lange, SYASL Partners*)
- (2) Receive an update on [SB 1166](#) ([Dodd – D](#)) an Act relating to postsecondary education, and consider making a recommendation (*Recommended by Supervisor Monica Brown, presented by Karen Lange, SYASL Partners*)
- (3) Receive an update from staff on the Solano County Legislative Committee 2024 meeting calendar and make a recommendation (*Presented by Matthew Davis, County Administrator's Office*)

(8) – POTENTIAL FUTURE SCHEDULED MEETINGS (*pending BOS approval of calendar*)

- (1) Monday, April 15, 2024 starting at 1:30 p.m.
- (2) Monday, June 3, 2024 starting at 1:30 p.m.
- (3) Monday, June 17, 2024 starting at 1:30 p.m.

(9) ADJOURN

ASSEMBLY BILL

No. 1957

Introduced by Assembly Member Wilson

January 29, 2024

An act to amend Sections 20155 and 20155.1 of, to amend the heading of Article 3.7 (commencing with Section 20155) of Chapter 1 of Part 3 of Division 2 of, and to repeal Sections 20155.7 and 20155.9 of, the Public Contract Code, relating to public contracts.

LEGISLATIVE COUNSEL'S DIGEST

AB 1957, as introduced, Wilson. Public contracts: best value construction contracting for counties.

Existing law establishes a pilot program to allow the Counties of Alameda, Los Angeles, Monterey, Riverside, San Bernardino, San Diego, San Mateo, Santa Clara, Solano, and Yuba to select a bidder on the basis of best value, as defined, for construction projects in excess of \$1,000,000. Existing law also authorizes these counties to use a best value construction contracting method to award individual annual contracts, not to exceed \$3,000,000, for repair, remodeling, or other repetitive work to be done according to unit prices, as specified. Existing law establishes procedures and criteria for the selection of a best value contractor and requires that bidders verify specified information under oath. Existing law requires the board of supervisors of a participating county to submit a report that contains specified information about the projects awarded using the best value procedures described above to the appropriate policy committees of the Legislature and the Joint Legislative Budget Committee before March 1, 2024. Existing law repeals the pilot program provisions on January 1, 2025.

This bill would instead authorize any county of the state to utilize this program and would remove the January 1, 2025, sunset date, thereby extending the operation of those provisions indefinitely. The bill would delete the requirement for the board of supervisors of a participating county to submit the report described above to the appropriate policy committees of the Legislature and the Joint Legislative Budget Committee before March 1, 2024. Because the bill would expand the program to all counties within the state and would indefinitely extend the operation of the program, the bill would expand the crime of perjury, thereby imposing a state-mandated local program.

The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.

This bill would provide that no reimbursement is required by this act for a specified reason.

Vote: majority. Appropriation: no. Fiscal committee: yes.
State-mandated local program: yes.

The people of the State of California do enact as follows:

1 SECTION 1. The heading of Article 3.7 (commencing with
2 Section 20155) of Chapter 1 of Part 3 of Division 2 of the Public
3 Contract Code is amended to read:

4
5 Article 3.7. Best Value Construction Contracting for Counties
6 Pilot Program
7

8 SEC. 2. Section 20155 of the Public Contract Code is amended
9 to read:

10 20155. (a) This article provides for a ~~pilot~~ *best value*
11 *procurement* program for the Counties of Alameda, Los Angeles,
12 Monterey, Riverside, San Bernardino, San Diego, San Mateo,
13 Santa Clara, Solano, and Yuba for *county* construction projects in
14 excess of one million dollars (\$1,000,000).

15 (b) The board of supervisors of a county shall let any contract
16 for a construction project pursuant to this article to the bidder
17 representing the best value or else reject all bids.

18 (c) The bidder may be selected on the basis of the best value to
19 the county. In order to implement this method of selection, the
20 board of supervisors shall adopt and publish procedures and

1 required criteria that ensure that all selections are conducted in a
2 fair and impartial manner. These procedures shall conform to
3 Sections 20155.3 to 20155.6, inclusive, and shall be mandatory
4 for a county that chooses to participate in the pilot program.

5 (d) If the board of supervisors of a county deems it to be in the
6 best interest of the county, the board of supervisors, on the refusal
7 or failure of the successful bidder for a project to execute a tendered
8 contract, may award it to the bidder with the second lowest best
9 value score, as determined in accordance with subdivision (c) of
10 Section 20155.5. If the second bidder fails or refuses to execute
11 the contract, the board of supervisors may likewise award it to the
12 bidder with the third lowest best value score, as determined in
13 accordance with subdivision (c) of Section 20155.5.

14 (e) (1) A county ~~listed in subdivision (a)~~ may also use the best
15 value construction contracting method set out in this article to
16 award individual annual contracts, which shall not exceed three
17 million dollars (\$3,000,000), adjusted annually to reflect the
18 percentage change in the California Consumer Price Index, for
19 repair, remodeling, or other repetitive work to be done according
20 to unit prices. The contracts shall be based on plans and
21 specifications for typical work. No annual contracts may be
22 awarded for any new construction.

23 (2) For purposes of this subdivision, best value criteria shall be
24 applied to the annual contract for construction services, rather than
25 to an individual, specific project. Annual contracts may be extended
26 or renewed for two subsequent annual terms and a maximum of
27 six million dollars (\$6,000,000) over the subsequent two terms of
28 the contract. Contract values shall be adjusted annually to reflect
29 the percentage change in the California Consumer Price Index.

30 (3) For purposes of this subdivision, “unit price” means the
31 amount paid for a single unit of an item of work, and “typical
32 work” means a work description applicable universally or
33 applicable to a large number of individual projects, as distinguished
34 from work specifically described with respect to an individual
35 project. For purposes of this section, “repair, remodeling, or other
36 repetitive work to be done according to unit prices” shall not
37 include design or contract drawings.

38 SEC. 3. Section 20155.1 of the Public Contract Code is
39 amended to read:

40 20155.1. As used in this article:

- 1 (a) “Best value” means a procurement process whereby the
 2 selected bidder may be selected on the basis of objective criteria
 3 for evaluating the qualifications of bidders with the resulting
 4 selection representing the best combination of price and
 5 qualifications.
- 6 (b) “Best value contract” means a competitively bid contract
 7 entered into pursuant to this article.
- 8 (c) “Best value contractor” means a properly licensed person,
 9 firm, or corporation that submits a bid for, or is awarded, a best
 10 value contract.
- 11 ~~(d) “County” means any of the following counties:~~
 12 ~~(1) The County of Alameda.~~
 13 ~~(2) The County of Los Angeles.~~
 14 ~~(3) The County of Monterey.~~
 15 ~~(4) The County of Riverside.~~
 16 ~~(5) The County of San Bernardino.~~
 17 ~~(6) The County of San Diego.~~
 18 ~~(7) The County of San Mateo.~~
 19 ~~(8) The County of Santa Clara.~~
 20 ~~(9) The County of Solano.~~
 21 ~~(10) The County of Yuba.~~
- 22 *(d) “County” means any chartered or general law county.*
 23 *“County” includes a city and county.*
- 24 (e) “Demonstrated management competency” means the
 25 experience, competency, capability, and capacity of the proposed
 26 management staffing to complete projects of similar size, scope,
 27 or complexity.
- 28 (f) “Financial condition” means the financial resources needed
 29 to perform the contract. The criteria used to evaluate a bidder’s
 30 financial condition shall include, at a minimum, capacity to obtain
 31 all required payment bonds, performance bonds, and liability
 32 insurance.
- 33 (g) “Labor compliance” means the ability to comply with, and
 34 past performance with, contract and statutory requirements for the
 35 payment of wages and qualifications of the workforce. The criteria
 36 used to evaluate a bidder’s labor compliance shall include, as a
 37 minimum, the bidder’s ability to comply with the apprenticeship
 38 requirements of the California Apprenticeship Council and the
 39 Department of Industrial Relations, its past conformance with

1 those requirements, and its past conformance with requirements
2 to pay prevailing wages on public works projects.

3 (h) “Qualifications” means the financial condition, relevant
4 experience, demonstrated management competency, labor
5 compliance, and safety record of the bidder, and, if required by
6 the bidding documents, some or all of the preceding qualifications
7 as they pertain to subcontractors proposed to be used by the bidder
8 for designated portions of the work. A county shall evaluate
9 financial condition, relevant experience, demonstrated management
10 competency, labor compliance, and safety record, using, to the
11 extent possible, quantifiable measurements.

12 (i) “Relevant experience” means the experience, competency,
13 capability, and capacity to complete projects of similar size, scope,
14 or complexity.

15 (j) “Safety record” means the prior history concerning the safe
16 performance of construction contracts. The criteria used to evaluate
17 a bidder’s safety record shall include, at a minimum, its experience
18 modification rate for the most recent three-year period, and its
19 average total recordable injury or illness rate and average lost work
20 rate for the most recent three-year period.

21 SEC. 4. Section 20155.7 of the Public Contract Code is
22 repealed.

23 ~~20155.7. (a) Before March 1, 2024, the board of supervisors~~
24 ~~of a participating county shall submit a report to the appropriate~~
25 ~~policy committees of the Legislature and the Joint Legislative~~
26 ~~Budget Committee. The report shall include, but is not limited to,~~
27 ~~the following information:~~

28 ~~(1) A description of the projects awarded using the best value~~
29 ~~procedures.~~

30 ~~(2) The contract award amounts.~~

31 ~~(3) The best value contractors awarded the projects.~~

32 ~~(4) A description of any written protests concerning any aspect~~
33 ~~of the solicitation, bid, or award of the best value contracts,~~
34 ~~including the resolution of the protests.~~

35 ~~(5) A description of the prequalification process.~~

36 ~~(6) The criteria used to evaluate the bids, including the weighting~~
37 ~~of the criteria and an assessment of the effectiveness of the~~
38 ~~methodology.~~

1 ~~(7) If a project awarded under this article has been completed,~~
2 ~~an assessment of the project performance, to include a summary~~
3 ~~of any delays or cost increases.~~

4 ~~(b) A report submitted pursuant to subdivision (a) shall be~~
5 ~~submitted in compliance with Section 9795 of the Government~~
6 ~~Code.~~

7 SEC. 5. Section 20155.9 of the Public Contract Code is
8 repealed.

9 ~~20155.9. This article shall remain in effect only until January~~
10 ~~1, 2025, and as of that date is repealed.~~

11 SEC. 6. No reimbursement is required by this act pursuant to
12 Section 6 of Article XIII B of the California Constitution because
13 the only costs that may be incurred by a local agency or school
14 district will be incurred because this act creates a new crime or
15 infraction, eliminates a crime or infraction, or changes the penalty
16 for a crime or infraction, within the meaning of Section 17556 of
17 the Government Code, or changes the definition of a crime within
18 the meaning of Section 6 of Article XIII B of the California
19 Constitution.

AMENDED IN SENATE AUGUST 14, 2023
AMENDED IN SENATE JULY 3, 2023
AMENDED IN ASSEMBLY APRIL 25, 2023
AMENDED IN ASSEMBLY APRIL 13, 2023
AMENDED IN ASSEMBLY MARCH 14, 2023
CALIFORNIA LEGISLATURE—2023–24 REGULAR SESSION

ASSEMBLY BILL

No. 749

Introduced by Assembly Member Irwin

February 13, 2023

An act to add Section 11549.45 to the Government Code, relating to state government.

LEGISLATIVE COUNSEL'S DIGEST

AB 749, as amended, Irwin. State agencies: information security: uniform standards.

Existing law establishes the Office of Information Security within the Department of Technology for the purpose of ensuring the confidentiality, integrity, and availability of state systems and applications and to promote and protect privacy as part of the development and operations of state systems and applications to ensure the trust of the residents of this state. The law requires state entities, as specified, to implement the policies and procedures issued by the office. The law additionally authorizes the office, under direction of the chief, to conduct, or require to be conducted, an independent security assessment of every state agency, department, or office, as specified. State agencies must certify, by February 1 annually, to the President

pro Tempore of the Senate and the Speaker of the Assembly that the agency is in compliance with all adopted policies, standards, and procedures and to include a plan of action and milestones, as specified.

This bill would require every state agency, as ~~defined~~, *defined and subject to specified exceptions*, to implement Zero Trust architecture for all data, hardware, software, internal systems, and essential third-party software, including for on-premises, cloud, and hybrid environments, to achieve prescribed levels of maturity based on the Cybersecurity and Infrastructure Security Agency (CISA) Maturity Model, as defined, by specified dates. In implementing Zero Trust architecture, the bill would require state agencies to prioritize the use of solutions that comply with, are authorized by, or align to federal guidelines, programs, and frameworks and, at a minimum, prioritize multifactor authentication for access to all systems and data, enterprise endpoint detection and response solutions, and robust logging practices, as specified. The bill would require the office's chief, no later than January 1, 2025, to develop or revise uniform technology policies, standards, and procedures for use by all state agencies in Zero Trust architecture to achieve specified maturity levels on all systems in the State Administrative Manual and Statewide Information Management Manual. The bill would require the chief to update requirements for existing annual reporting activities to collect information relating to the progress state agencies are making to increase internal defenses of agency systems. The bill would authorize the chief to update existing annual reporting activities to include how a state agency is progressing with respect to specified goals. The bill would also state the Legislature's intent that the bill's provisions be implemented in a manner consistent with the state's timely compliance with requirements that are conditions to receipt of federal funds. The bill would also make related legislative findings and declarations.

Vote: majority. Appropriation: no. Fiscal committee: yes.
State-mandated local program: no.

The people of the State of California do enact as follows:

- 1 SECTION 1. The Legislature finds and declares the following:
- 2 (a) Recent cyber breaches have had wide-ranging consequences
- 3 and demand a state-level response. Cyber defense requires greater
- 4 speed and agility to mitigate cyber threats, limit the impact of data
- 5 breaches, and better protect the state's workforce and residents.

1 These attacks not only significantly impact institutions financially,
2 but they also erode public trust and confidence in government.

3 (b) To better defend against cyber threats, the Legislature intends
4 for state agencies to embrace technologies and practices outlined
5 in Executive Order 14028 on Improving the Nation's
6 Cybersecurity. At a minimum, this includes formalizing Zero Trust
7 as the desired model for security. Zero Trust is a security
8 architecture requiring all users, whether in or outside the
9 organization's network, to be authenticated, authorized, and
10 continuously validated for security configuration and posture before
11 being granted or retaining access to applications and data.

12 SEC. 2. Section 11549.45 is added to the Government Code,
13 to read:

14 11549.45. (a) For purposes of this section, the following
15 definitions shall apply:

16 (1) "Chief" means the Chief of the Office of Information
17 Security.

18 (2) "Cybersecurity and Infrastructure Security Agency (CISA)
19 Maturity Model" means the Zero Trust Maturity Model published
20 by the Cybersecurity and Infrastructure Security Agency.

21 (3) "Endpoint detection and response" means a cybersecurity
22 solution that continuously monitors end-user devices to detect and
23 respond to cyber threats.

24 (4) "Multifactor authentication" means using two or more
25 different types of identification factors to authenticate a user's
26 identity for the purpose of accessing systems and data.

27 (5) "State agency" has the same meaning as in Section 11000.

28 (6) "Zero Trust architecture" means a security model, a set of
29 system design principles, and a coordinated cybersecurity and
30 system management strategy that employs continuous monitoring,
31 risk-based access controls, secure identity and access management
32 practices, and system security automation techniques to address
33 the cybersecurity risk from threats inside and outside traditional
34 network boundaries.

35 (b) Every state agency shall implement Zero Trust architecture
36 for all data, hardware, software, internal systems, and essential
37 third-party software, including for on-premises, cloud, and hybrid
38 environments, according to the following levels of maturity based
39 upon the Cybersecurity and Infrastructure Security Agency (CISA)
40 Maturity Model:

1 (1) Achieve “Initial” maturity by June 1, 2024.

2 (2) Achieve “Advanced” maturity by June 1, 2026.

3 (3) Achieve “Optimal” maturity by June 1, 2030.

4 (c) In implementing Zero Trust architecture, a state agency shall
5 prioritize the use of solutions that comply with, are authorized by,
6 or align to applicable federal guidelines, programs, and
7 frameworks, including the Federal Risk and Authorization
8 Management Program, the Continuous Diagnostics and Mitigation
9 Program, and guidance and frameworks from the National Institute
10 of Standards and Technology.

11 (d) Implementation shall, at a minimum, prioritize the following:

12 (1) Multifactor authentication for access to all systems and data
13 owned, managed, maintained, or utilized by or on behalf of the
14 state agency.

15 (2) Enterprise endpoint detection and response solutions to
16 promote real-time detection of cybersecurity threats and rapid
17 investigation and remediation capabilities.

18 (3) Robust logging practices to provide adequate data to support
19 security investigations and proactive threat hunting.

20 (e) No later than January 1, 2025, the chief shall develop or
21 revise uniform technology policies, standards, and procedures for
22 use by each state agency in implementing Zero Trust architecture
23 to achieve the “Advanced” and “Optimal” maturity levels stated
24 in subdivision (b) in the State Administrative Manual and Statewide
25 Information Management Manual. A state agency subject to
26 subdivision (f) of Section 11549.3 may, but is not required to, use
27 the policies, standards, and procedures developed by the chief.

28 (f) The chief shall update requirements for existing annual
29 reporting activities, including standards for audits and independent
30 security assessments, to collect information relating to a state
31 agency’s progress in increasing the internal defenses of agency
32 systems, including:

33 (1) A description of any steps the state agency has completed,
34 including advancements toward achieving Zero Trust architecture
35 maturity levels.

36 (2) Following an independent security assessment, an
37 identification of activities that have not yet been completed and
38 that would have the most immediate security impact.

39 (3) A schedule to implement any planned activities.

1 (g) The chief may update requirements for existing annual
2 reporting activities, including standards for audits and independent
3 security assessments, to also include information on how a state
4 agency is progressing with respect to the following:

5 (1) Shifting away from trusted networks to implement security
6 controls based on a presumption of compromise.

7 (2) Implementing principles of least privilege in administering
8 information security programs.

9 (3) Limiting the ability of entities that cause cyberattacks to
10 move laterally through or between a state agency's systems.

11 (4) Identifying cyber threats quickly.

12 (5) Isolating and removing unauthorized entities from state
13 agencies' systems as quickly as practicable, accounting for cyber
14 threat intelligence or law enforcement purposes.

15 (h) *This section shall apply to the University of California only*
16 *to the extent that the Regents of the University of California, by*
17 *resolution, make any of these provisions applicable to the*
18 *university.*

19 ~~(h)~~

20 (i) It is the intent of the Legislature that this section be
21 implemented in a manner that is consistent with the state's timely
22 compliance with requirements that are conditions to receipt of
23 federal funds, including, but not limited to, funding from the
24 Infrastructure Investment and Jobs Act (Public Law 117-58).

Introduced by Senator WienerFebruary 7, 2024

An act to add Chapter 22.6 (commencing with Section 22602) to Division 8 of the Business and Professions Code, and to add Sections 11547.6 and 11547.7 to the Government Code, relating to artificial intelligence.

LEGISLATIVE COUNSEL'S DIGEST

SB 1047, as introduced, Wiener. Safe and Secure Innovation for Frontier Artificial Intelligence Systems Act.

Existing law requires the Secretary of Government Operations to develop a coordinated plan to, among other things, investigate the feasibility of, and obstacles to, developing standards and technologies for state departments to determine digital content provenance. For the purpose of informing that coordinated plan, existing law requires the secretary to evaluate, among other things, the impact of the proliferation of deepfakes, defined to mean audio or visual content that has been generated or manipulated by artificial intelligence that would falsely appear to be authentic or truthful and that features depictions of people appearing to say or do things they did not say or do without their consent, on state government, California-based businesses, and residents of the state.

Existing law creates the Department of Technology within the Government Operations Agency and requires the department to, among other things, identify, assess, and prioritize high-risk, critical information technology services and systems across state government for modernization, stabilization, or remediation.

This bill would enact the Safe and Secure Innovation for Frontier Artificial Intelligence Systems Act to, among other things, require a

developer of a covered model, as defined, to determine whether it can make a positive safety determination with respect to a covered model before initiating training of that covered model, as specified. The bill would define “positive safety determination” to mean a determination with respect to a covered model, that is not a derivative model, that a developer can reasonably exclude the possibility that the covered model has a hazardous capability, as defined, or may come close to possessing a hazardous capability when accounting for a reasonable margin for safety and the possibility of posttraining modifications.

This bill would require that a developer, before initiating training of a nonderivative covered model, comply with various requirements, including implementing the capability to promptly enact a full shutdown of the covered model until that covered model is the subject of a positive safety determination.

This bill would require a developer of a nonderivative covered model that is not the subject of a positive safety determination to submit to the Frontier Model Division, which the bill would create within the Department of Technology, an annual certification of compliance with these provisions signed by the chief technology officer, or a more senior corporate officer, in a format and on a date as prescribed by the Frontier Model Division. By expanding the scope of the crime of perjury, this bill would impose a state-mandated local program. The bill would also require a developer to report each artificial intelligence safety incident affecting a covered model to the Frontier Model Division in a manner prescribed by the Frontier Model Division.

This bill would require a person that operates a computing cluster, as defined, to implement appropriate written policies and procedures to do certain things when a customer utilizes compute resources that would be sufficient to train a covered model, including assess whether a prospective customer intends to utilize the computing cluster to deploy a covered model. The bill would punish a violation of these provisions with a civil penalty, as prescribed, to be recovered by the Attorney General.

This bill would also create the Frontier Model Division within the Department of Technology and would require the division to, among other things, review annual certification reports from developers received pursuant to these provisions and publicly release summarized findings based on those reports. The bill would authorize the division to assess related fees and would require deposit of the fees into the Frontier Model Division Programs Fund, which the bill would create.

The bill would make moneys in the fund available for the purpose of these provisions only upon appropriation by the Legislature.

This bill would also require the Department of Technology to commission consultants, as prescribed, to create a public cloud computing cluster, to be known as CalCompute, with the primary focus of conducting research into the safe and secure deployment of large-scale artificial intelligence models and fostering equitable innovation that includes, among other things, a fully owned and hosted cloud platform.

The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.

This bill would provide that no reimbursement is required by this act for a specified reason.

Vote: majority. Appropriation: no. Fiscal committee: yes.
State-mandated local program: yes.

The people of the State of California do enact as follows:

- 1 SECTION 1. This act shall be known, and may be cited, as the
- 2 Safe and Secure Innovation for Frontier Artificial Intelligence
- 3 Systems Act.
- 4 SEC. 2. The Legislature finds and declares all of the following:
- 5 (a) California is leading the world in artificial intelligence
- 6 innovation and research, through companies large and small, as
- 7 well as through our remarkable public and private universities.
- 8 (b) Artificial intelligence, including new advances in generative
- 9 artificial intelligence, has the potential to catalyze innovation and
- 10 the rapid development of a wide range of benefits for Californians
- 11 and the California economy, including advances in medicine,
- 12 wildfire forecasting and prevention, and climate science, and to
- 13 push the bounds of human creativity and capacity.
- 14 (c) If not properly subject to human controls, future development
- 15 in artificial intelligence may also have the potential to be used to
- 16 create novel threats to public safety and security, including by
- 17 enabling the creation and the proliferation of weapons of mass
- 18 destruction, such as biological, chemical, and nuclear weapons,
- 19 as well as weapons with cyber-offensive capabilities.
- 20 (d) The state government has an essential role to play in ensuring
- 21 that California recognizes the benefits of this technology while
- 22 avoiding the most severe risks, as well as to ensure that artificial

1 intelligence innovation and access to compute is accessible to
2 academic researchers and startups, in addition to large companies.
3 SEC. 3. Chapter 22.6 (commencing with Section 22602) is
4 added to Division 8 of the Business and Professions Code, to read:

5
6 CHAPTER 22.6. SAFE AND SECURE INNOVATION FOR FRONTIER
7 ARTIFICIAL INTELLIGENCE SYSTEMS

8
9 22602. As used in this chapter:

10 (a) “Advanced persistent threat” means an adversary with
11 sophisticated levels of expertise and significant resources that
12 allow it, through the use of multiple different attack vectors,
13 including, but not limited to, cyber, physical, and deception, to
14 generate opportunities to achieve its objectives that are typically
15 to establish and extend its presence within the information
16 technology infrastructure of organizations for purposes of
17 exfiltrating information or to undermine or impede critical aspects
18 of a mission, program, or organization or place itself in a position
19 to do so in the future.

20 (b) “Artificial intelligence model” means a machine-based
21 system that can make predictions, recommendations, or decisions
22 influencing real or virtual environments and can use model
23 inference to formulate options for information or action.

24 (c) “Artificial intelligence safety incident” means any of the
25 following:

26 (1) A covered model autonomously engaging in a sustained
27 sequence of unsafe behavior other than at the request of a user.

28 (2) Theft, misappropriation, malicious use, inadvertent release,
29 unauthorized access, or escape of the model weights of a covered
30 model.

31 (3) The critical failure of technical or administrative controls,
32 including controls limiting the ability to modify a covered model,
33 designed to limit access to a hazardous capability of a covered
34 model.

35 (4) Unauthorized use of the hazardous capability of a covered
36 model.

37 (d) “Computing cluster” means a set of machines transitively
38 connected by data center networking of over 100 gigabits that has
39 a theoretical maximum computing capacity of 10^{20} integer or

1 floating-point operations per second for training artificial
2 intelligence.

3 (e) “Covered guidance” means any of the following:

4 (1) Applicable guidance issued by the National Institute of
5 Standards and Technology and by the Frontier Model Division.

6 (2) Industry best practices, including relevant safety practices,
7 precautions, or testing procedures undertaken by developers of
8 comparable models, and any safety standards or best practices
9 commonly or generally recognized by relevant experts in academia
10 or the nonprofit sector.

11 (3) Applicable safety-enhancing standards set by standards
12 setting organizations.

13 (f) “Covered model” means an artificial intelligence model that
14 meets either of the following criteria:

15 (1) The artificial intelligence model was trained using a quantity
16 of computing power greater than 10^{26} integer or floating-point
17 operations in 2024, or a model that could reasonably be expected
18 to have similar performance on benchmarks commonly used to
19 quantify the performance of state-of-the-art foundation models,
20 as determined by industry best practices and relevant standard
21 setting organizations.

22 (2) The artificial intelligence model has capability below the
23 relevant threshold on a specific benchmark but is of otherwise
24 similar general capability.

25 (g) “Critical harm” means a harm listed in paragraph (1) of
26 subdivision (n).

27 (h) “Critical infrastructure” means assets, systems, and networks,
28 whether physical or virtual, the incapacitation or destruction of
29 which would have a debilitating effect on physical security,
30 economic security, public health, or safety in the state.

31 (i) (1) “Derivative model” means an artificial intelligence model
32 that is a derivative of another artificial intelligence model, including
33 either of the following:

34 (A) A modified or unmodified copy of an artificial intelligence
35 model.

36 (B) A combination of an artificial intelligence model with other
37 software.

38 (2) “Derivative model” does not include an entirely
39 independently trained artificial intelligence model.

- 1 (j) (1) “Developer” means a person that creates, owns, or
2 otherwise has responsibility for an artificial intelligence model.
- 3 (2) “Developer” does not include a third-party machine-learning
4 operations platform, an artificial intelligence infrastructure
5 platform, a computing cluster, an application developer using
6 sourced models, or an end-user of an artificial intelligence model.
- 7 (k) “Fine tuning” means the adjustment of the model weights
8 of an artificial intelligence model that has been previously trained
9 by training the model with new data.
- 10 (l) “Frontier Model Division” means the Frontier Model Division
11 created pursuant to Section 11547.6 of the Government Code.
- 12 (m) “Full shutdown” means the cessation of operation of a
13 covered model, including all copies and derivative models, on all
14 computers and storage devices within custody, control, or
15 possession of a person, including any computer or storage device
16 remotely provided by agreement.
- 17 (n) (1) “Hazardous capability” means the capability of a covered
18 model to be used to enable any of the following harms in a way
19 that would be significantly more difficult to cause without access
20 to a covered model:
- 21 (A) The creation or use of a chemical, biological, radiological,
22 or nuclear weapon in a manner that results in mass casualties.
- 23 (B) At least five hundred million dollars (\$500,000,000) of
24 damage through cyberattacks on critical infrastructure via a single
25 incident or multiple related incidents.
- 26 (C) At least five hundred million dollars (\$500,000,000) of
27 damage by an artificial intelligence model that autonomously
28 engages in conduct that would violate the Penal Code if undertaken
29 by a human.
- 30 (D) Other threats to public safety and security that are of
31 comparable severity to the harms described in paragraphs (A) to
32 (C), inclusive.
- 33 (2) “Hazardous capability” includes a capability described in
34 paragraph (1) even if the hazardous capability would not manifest
35 but for fine tuning and posttraining modifications performed by
36 third-party experts intending to demonstrate those abilities.
- 37 (o) “Machine-learning operations platform” means a solution
38 that includes a combined offering of necessary machine-learning
39 development capabilities, including exploratory data analysis, data
40 preparation, model training and tuning, model review and

1 governance, model inference and serving, model deployment and
2 monitoring, and automated model retraining.

3 (p) “Model weight” means a numerical parameter established
4 through training in an artificial intelligence model that helps
5 determine how input information impacts a model’s output.

6 (q) “Open-source artificial intelligence model” means an
7 artificial intelligence model that is made freely available and may
8 be freely modified and redistributed.

9 (r) “Person” means an individual, proprietorship, firm,
10 partnership, joint venture, syndicate, business trust, company,
11 corporation, limited liability company, association, committee, or
12 any other nongovernmental organization or group of persons acting
13 in concert.

14 (s) “Positive safety determination” means a determination,
15 pursuant to subdivision (a) or (c) of Section 22603, with respect
16 to a covered model that is not a derivative model that a developer
17 can reasonably exclude the possibility that a covered model has a
18 hazardous capability or may come close to possessing a hazardous
19 capability when accounting for a reasonable margin for safety and
20 the possibility of posttraining modifications.

21 (t) “Posttraining modification” means the modification of the
22 capabilities of an artificial intelligence model after the completion
23 of training by any means, including, but not limited to, initiating
24 additional training, providing the model with access to tools or
25 data, removing safeguards against hazardous misuse or misbehavior
26 of the model, or combining the model with, or integrating it into,
27 other software.

28 (u) “Safety and security protocol” means documented technical
29 and organizational protocols that meet both of the following
30 criteria:

31 (1) The protocols are used to manage the risks of developing
32 and operating covered models across their life cycle, including
33 risks posed by enabling or potentially enabling the creation of
34 derivative models.

35 (2) The protocols specify that compliance with the protocols is
36 required in order to train, operate, possess, and provide external
37 access to the developer’s covered model.

38 22603. (a) Before initiating training of a covered model that
39 is not a derivative model, a developer of that covered model shall

1 determine whether it can make a positive safety determination
2 with respect to the covered model.

3 (1) In making the determination required by this subdivision, a
4 developer shall incorporate all covered guidance.

5 (2) A developer may make a positive safety determination if
6 the covered model will have lower performance on all benchmarks
7 relevant under subdivision (f) of Section 22602 than either of the
8 following:

9 (A) A non-covered model that manifestly lacks hazardous
10 capabilities.

11 (B) Another model that is the subject of a positive safety
12 determination.

13 (3) Upon making a positive safety determination, the developer
14 of the covered model shall submit to the Frontier Model Division
15 a certification under penalty of perjury that specifies the basis for
16 that conclusion.

17 (b) Before initiating training of a covered model that is not a
18 derivative model that is not the subject of a positive safety
19 determination, and until that covered model is the subject of a
20 positive safety determination, the developer of that covered model
21 shall do all of the following:

22 (1) Implement administrative, technical, and physical
23 cybersecurity protections to prevent unauthorized access to, or
24 misuse or unsafe modification of, the covered model, including to
25 prevent theft, misappropriation, malicious use, or inadvertent
26 release or escape of the model weights from the developer's
27 custody, that are appropriate in light of the risks associated with
28 the covered model, including from advanced persistent threats or
29 other sophisticated actors.

30 (2) Implement the capability to promptly enact a full shutdown
31 of the covered model.

32 (3) Implement all covered guidance.

33 (4) Implement a written and separate safety and security protocol
34 that does all of the following:

35 (A) Provides reasonable assurance that if a developer complies
36 with its safety and security protocol, either of the following will
37 apply:

38 (i) The developer will not produce a covered model with a
39 hazardous capability or enable the production of a derivative model
40 with a hazardous capability.

1 (ii) The safeguards enumerated in the policy will be sufficient
2 to prevent critical harms from the exercise of a hazardous capability
3 in a covered model.

4 (B) States compliance requirements in an objective manner and
5 with sufficient detail and specificity to allow the developer or a
6 third party to readily ascertain whether the requirements of the
7 safety and security protocol have been followed.

8 (C) Identifies specific tests and test results that would be
9 sufficient to reasonably exclude the possibility that a covered model
10 has a hazardous capability or may come close to possessing a
11 hazardous capability when accounting for a reasonable margin for
12 safety and the possibility of posttraining modifications, and in
13 addition does all of the following:

14 (i) Describes in detail how the testing procedure incorporates
15 fine tuning and posttraining modifications performed by third-party
16 experts intending to demonstrate those abilities.

17 (ii) Describes in detail how the testing procedure incorporates
18 the possibility of posttraining modifications.

19 (iii) Describes in detail how the testing procedure incorporates
20 the requirement for reasonable margin for safety.

21 (iv) Provides sufficient detail for third parties to replicate the
22 testing procedure.

23 (D) Describes in detail how the developer will meet
24 requirements listed under paragraphs (1), (2), (3), and (5).

25 (E) If applicable, describes in detail how the developer intends
26 to implement the safeguards and requirements referenced in
27 paragraph (1) of subdivision (d).

28 (F) Describes in detail the conditions that would require the
29 execution of a full shutdown.

30 (G) Describes in detail the procedure by which the safety and
31 security protocol may be modified.

32 (H) Meets other criteria stated by the Frontier Model Division
33 in guidance to achieve the purpose of maintaining the safety of a
34 covered model with a hazardous capability.

35 (5) Ensure that the safety and security protocol is implemented
36 as written, including, at a minimum, by designating senior
37 personnel responsible for ensuring implementation by employees
38 and contractors working on a covered model, monitoring and
39 reporting on implementation, and conducting audits, including
40 through third parties as appropriate.

1 (6) Provide a copy of the safety and security protocol to the
2 Frontier Model Division.

3 (7) Conduct an annual review of the safety and security protocol
4 to account for any changes to the capabilities of the covered model
5 and industry best practices and, if necessary, make modifications
6 to the policy.

7 (8) If the safety and security protocol is modified, provide an
8 updated copy to the Frontier Model Division within 10 business
9 days.

10 (9) Refrain from initiating training of a covered model if there
11 remains an unreasonable risk that an individual, or the covered
12 model itself, may be able to use the hazardous capabilities of the
13 covered model, or a derivative model based on it, to cause a critical
14 harm.

15 (c) (1) Upon completion of the training of a covered model that
16 is not the subject of a positive safety determination and is not a
17 derivative model, the developer shall perform capability testing
18 sufficient to determine whether the developer can make a positive
19 safety determination with respect to the covered model pursuant
20 to its safety and security protocol.

21 (2) Upon making a positive safety determination with respect
22 to the covered model, a developer of the covered model shall
23 submit to the Frontier Model Division a certification of compliance
24 with the requirements of this section within 90 days and no more
25 than 30 days after initiating the commercial, public, or widespread
26 use of the covered model that includes both of the following:

27 (A) The basis for the developer's positive safety determination.

28 (B) The specific methodology and results of the capability
29 testing undertaken pursuant to this subdivision.

30 (d) Before initiating the commercial, public, or widespread use
31 of a covered model that is not subject to a positive safety
32 determination, a developer of the nonderivative version of the
33 covered model shall do all of the following:

34 (1) Implement reasonable safeguards and requirements to do
35 all of the following:

36 (A) Prevent an individual from being able to use the hazardous
37 capabilities of the model, or a derivative model, to cause a critical
38 harm.

39 (B) Prevent an individual from being able to use the model to
40 create a derivative model that was used to cause a critical harm.

1 (C) Ensure, to the extent reasonably possible, that the covered
2 model’s actions and any resulting critical harms can be accurately
3 and reliably attributed to it and any user responsible for those
4 actions.

5 (2) Provide reasonable requirements to developers of derivative
6 models to prevent an individual from being able to use a derivative
7 model to cause a critical harm.

8 (3) Refrain from initiating the commercial, public, or widespread
9 use of a covered model if there remains an unreasonable risk that
10 an individual may be able to use the hazardous capabilities of the
11 model, or a derivative model based on it, to cause a critical harm.

12 (e) A developer of a covered model shall periodically reevaluate
13 the procedures, policies, protections, capabilities, and safeguards
14 implemented pursuant to this section in light of the growing
15 capabilities of covered models and as is reasonably necessary to
16 ensure that the covered model or its users cannot remove or bypass
17 those procedures, policies, protections, capabilities, and safeguards.

18 (f) (1) A developer of a nonderivative covered model that is
19 not the subject of a positive safety determination shall submit to
20 the Frontier Model Division an annual certification of compliance
21 with the requirements of this section signed by the chief technology
22 officer, or a more senior corporate officer, in a format and on a
23 date as prescribed by the Frontier Model Division.

24 (2) In a certification submitted pursuant to paragraph (1), a
25 developer shall specify or provide, at a minimum, all of the
26 following:

27 (A) The nature and magnitude of hazardous capabilities that the
28 covered model possesses or may reasonably possess and the
29 outcome of capability testing required by subdivision (c).

30 (B) An assessment of the risk that compliance with the safety
31 and security protocol may be insufficient to prevent harms from
32 the exercise of the covered model’s hazardous capabilities.

33 (C) Other information useful to accomplishing the purposes of
34 this subdivision, as determined by the Frontier Model Division.

35 (g) A developer shall report each artificial intelligence safety
36 incident affecting a covered model to the Frontier Model Division
37 in a manner prescribed by the Frontier Model Division. The
38 notification shall be made in the most expedient time possible and
39 without unreasonable delay and in no event later than 72 hours
40 after learning that an artificial intelligence safety incident has

1 occurred or learning facts sufficient to establish a reasonable belief
2 that an artificial intelligence safety incident has occurred.

3 (h) (1) Reliance on an unreasonable positive safety
4 determination does not relieve a developer of its obligations under
5 this section.

6 (2) A positive safety determination is unreasonable if the
7 developer does not take into account reasonably foreseeable risks
8 of harm or weaknesses in capability testing that lead to an
9 inaccurate determination.

10 (3) A risk of harm or weakness in capability testing is reasonably
11 foreseeable, if, by the time that a developer releases a model, an
12 applicable risk of harm or weakness in capability testing has
13 already been identified by either of the following:

14 (A) Any other developer of a comparable or comparably
15 powerful model through risk assessment, capability testing, or
16 other means.

17 (B) By the United States Artificial Intelligence Safety Institute,
18 the Frontier Model Division, or any independent standard-setting
19 organization or capability-testing organization cited by either of
20 those entities.

21 22604. A person that operates a computing cluster shall
22 implement appropriate written policies and procedures to do all
23 of the following when a customer utilizes compute resources that
24 would be sufficient to train a covered model:

25 (a) Obtain a prospective customer's basic identifying
26 information and business purpose for utilizing the computing
27 cluster, including all of the following:

28 (1) The identity of that prospective customer.

29 (2) The means and source of payment, including any associated
30 financial institution, credit card number, account number, customer
31 identifier, transaction identifiers, or virtual currency wallet or
32 wallet address identifier.

33 (3) The email address and telephonic contact information used
34 to verify a prospective customer's identity.

35 (4) The Internet Protocol addresses used for access or
36 administration and the date and time of each access or
37 administrative action.

38 (b) Assess whether a prospective customer intends to utilize the
39 computing cluster to deploy a covered model.

1 (c) Annually validate the information collected pursuant to
2 subdivision (a) and conduct the assessment required pursuant to
3 subdivision (b).

4 (d) Maintain for seven years and provide to the Frontier Model
5 Division or the Attorney General, upon request, appropriate records
6 of actions taken under this section, including policies and
7 procedures put into effect.

8 (e) Implement the capability to promptly enact a full shutdown
9 in the event of an emergency.

10 22605. (a) A developer of a covered model that provides
11 commercial access to that covered model shall provide a
12 transparent, uniform, publicly available price schedule for the
13 purchase of access to that covered model at a given level of quality
14 and quantity subject to the developer's terms of service and shall
15 not engage in unlawful discrimination or noncompetitive activity
16 in determining price or access.

17 (b) A person that operates a computing cluster shall provide a
18 transparent, uniform, publicly available price schedule for the
19 purchase of access to the computing cluster at a given level of
20 quality and quantity subject to the developer's terms of service
21 and shall not engage in unlawful discrimination or noncompetitive
22 activity in determining price or access.

23 22606. (a) If the Attorney General has reasonable cause to
24 believe that a person is violating this chapter, the Attorney General
25 shall commence a civil action in a court of competent jurisdiction.

26 (b) In a civil action under this section, the court may award any
27 of the following:

28 (1) (A) Preventive relief, including a permanent or temporary
29 injunction, restraining order, or other order against the person
30 responsible for a violation of this chapter, including deletion of
31 the covered model and the weights utilized in that model.

32 (B) Relief pursuant to this paragraph shall be granted only in
33 response to harm or an imminent risk or threat to public safety.

34 (2) Other relief as the court deems appropriate, including
35 monetary damages to persons aggrieved and an order for the full
36 shutdown of a covered model.

37 (3) A civil penalty in an amount not exceeding 10 percent of
38 the cost, excluding labor cost, to develop the covered model for a
39 first violation and in an amount not exceeding 30 percent of the

1 cost, excluding labor cost, to develop the covered model for any
2 subsequent violation.

3 (c) In the apportionment of penalties assessed pursuant to this
4 section, defendants shall be jointly and severally liable.

5 (d) A court shall disregard corporate formalities and impose
6 joint and several liability on affiliated entities for purposes of
7 effectuating the intent of this section if the court concludes that
8 both of the following are true:

9 (1) Steps were taken in the development of the corporate
10 structure among affiliated entities to purposely and unreasonably
11 limit or avoid liability.

12 (2) The corporate structure of the developer or affiliated entities
13 would frustrate recovery of penalties or injunctive relief under this
14 section.

15 22607. (a) Pursuant to subdivision (a) of Section 1102.5 of
16 the Labor Code, a developer shall not prevent an employee from
17 disclosing information to the Attorney General if the employee
18 has reasonable cause to believe that the information indicates that
19 the developer is out of compliance with the requirements of Section
20 22603.

21 (b) Pursuant to subdivision (b) of Section 1102.5 of the Labor
22 Code, a developer shall not retaliate against an employee for
23 disclosing information to the Attorney General if the employee
24 has reasonable cause to believe that the information indicates that
25 the developer is out of compliance with the requirements of Section
26 22603.

27 (c) The Attorney General may publicly release any complaint,
28 or a summary of that complaint, pursuant to this section if the
29 Attorney General concludes that doing so will serve the public
30 interest.

31 (d) Employees shall seek relief for violations of this section
32 pursuant to Sections 1102.61 and 1102.62 of the Labor Code.

33 (e) Pursuant to subdivision (a) of Section 1102.8 of the Labor
34 Code, a developer shall provide clear notice to all employees
35 working on covered models of their rights and responsibilities
36 under this section.

37 SEC. 4. Section 11547.6 is added to the Government Code, to
38 read:

39 11547.6. (a) As used in this section:

1 (1) “Hazardous capability” has the same meaning as defined in
2 Section 22602 of the Business and Professions Code.

3 (2) “Positive safety determination” has the same meaning as
4 defined in Section 22602 of the Business and Professions Code.

5 (b) The Frontier Model Division is hereby created within the
6 Department of Technology.

7 (c) The Frontier Model Division shall do all of the following:

8 (1) Review annual certification reports received from developers
9 pursuant to Section 22603 of the Business and Professions Code
10 and publicly release summarized findings based on those reports.

11 (2) Advise the Attorney General on potential violations of this
12 section or Chapter 22.6 (commencing with Section 22602) of
13 Division 8 of the Business and Professions Code.

14 (3) (A) Issue guidance, standards, and best practices sufficient
15 to prevent unreasonable risks from covered models with hazardous
16 capabilities including, but not limited to, more specific
17 requirements on the duties required under Section 22603 of the
18 Business and Professions Code.

19 (B) Establish an accreditation process and relevant accreditation
20 standards under which third parties may be accredited for a
21 three-year period, which may be extended through an appropriate
22 process, to certify adherence by developers to the best practices
23 and standards adopted pursuant to subparagraph (A).

24 (4) Publish anonymized artificial intelligence safety incident
25 reports received from developers pursuant to Section 22603 of the
26 Business and Professions Code.

27 (5) Establish confidential fora that are structured and facilitated
28 in a manner that allows developers to share best risk management
29 practices for models with hazardous capabilities in a manner
30 consistent with state and federal antitrust laws.

31 (6) (A) Issue guidance describing the categories of artificial
32 intelligence safety events that are likely to constitute a state of
33 emergency within the meaning of subdivision (b) of Section 8558
34 and responsive actions that could be ordered by the Governor after
35 a duly proclaimed state of emergency.

36 (B) The guidance issued pursuant to subparagraph (A) shall not
37 limit, modify, or restrict the authority of the Governor in any way.

38 (7) Appoint and consult with an advisory committee that shall
39 advise the Governor on when it may be necessary to proclaim a

1 state of emergency relating to artificial intelligence and advise the
2 Governor on what responses may be appropriate in that event.

3 (8) Appoint and consult with an advisory committee for
4 open-source artificial intelligence that shall do all of the following:

5 (A) Issue guidelines for model evaluation for use by developers
6 of open-source artificial intelligence models that do not have
7 hazardous capabilities.

8 (B) Advise the Frontier Model Division on the creation and
9 feasibility of incentives, including tax credits, that could be
10 provided to developers of open-source artificial intelligence models
11 that are not covered models.

12 (C) Advise the Frontier Model Division on future policies and
13 legislation impacting open-source artificial intelligence
14 development.

15 (9) Provide technical assistance and advice to the Legislature,
16 upon request, with respect to artificial intelligence-related
17 legislation.

18 (10) Monitor relevant developments relating to the safety risks
19 associated with the development of artificial intelligence models
20 and the functioning of markets for artificial intelligence models.

21 (11) Levy fees, including an assessed fee for the submission of
22 a certification, in an amount sufficient to cover the reasonable
23 costs of administering this section that do not exceed the reasonable
24 costs of administering this section.

25 (12) (A) Develop and submit to the Judicial Council proposed
26 model jury instructions for actions brought by individuals injured
27 by a hazardous capability of a covered model.

28 (B) In developing the model jury instructions required by
29 subparagraph (A), the Frontier Model Division shall consider all
30 of the following factors:

31 (i) The level of rigor and detail of the safety and security
32 protocol that the developer faithfully implemented while it trained,
33 stored, and released a covered model.

34 (ii) Whether and to what extent the developer's safety and
35 security protocol was inferior, comparable, or superior, in its level
36 of rigor and detail, to the mandatory safety policies of comparable
37 developers.

38 (iii) The extent and quality of the developer's safety and security
39 protocol's prescribed safeguards, capability testing, and other

1 precautionary measures with respect to the relevant hazardous
2 capability and related hazardous capabilities.

3 (iv) Whether and to what extent the developer and its agents
4 complied with the developer’s safety and security protocol, and
5 to the full degree, that doing so might plausibly have avoided
6 causing a particular harm.

7 (v) Whether and to what extent the developer carefully and
8 rigorously investigated, documented, and accurately measured,
9 insofar as reasonably possible given the state of the art, relevant
10 risks that its model might pose.

11 (d) There is hereby created in the General Fund the Frontier
12 Model Division Programs Fund.

13 (1) All fees received by the Frontier Model Division pursuant
14 to this section shall be deposited into the fund.

15 (2) All moneys in the account shall be available, only upon
16 appropriation by the Legislature, for purposes of carrying out the
17 provisions of this section.

18 SEC. 5. Section 11547.7 is added to the Government Code, to
19 read:

20 11547.7. (a) The Department of Technology shall commission
21 consultants, pursuant to subdivision (b), to create a public cloud
22 computing cluster, to be known as CalCompute, with the primary
23 focus of conducting research into the safe and secure deployment
24 of large-scale artificial intelligence models and fostering equitable
25 innovation that includes, but is not limited to, all of the following:

26 (1) A fully owned and hosted cloud platform.

27 (2) Necessary human expertise to operate and maintain the
28 platform.

29 (3) Necessary human expertise to support, train, and facilitate
30 use of CalCompute.

31 (b) The consultants shall include, but not be limited to,
32 representatives of national laboratories, public universities, and
33 any relevant professional associations or private sector
34 stakeholders.

35 (c) To meet the objective of establishing CalCompute, the
36 Department of Technology shall require consultants commissioned
37 to work on this process to evaluate and incorporate all of the
38 following considerations into its plan:

39 (1) An analysis of the public, private, and nonprofit cloud
40 platform infrastructure ecosystem, including, but not limited to,

1 dominant cloud providers, the relative compute power of each
2 provider, the estimated cost of supporting platforms as well as
3 pricing models, and recommendations on the scope of CalCompute.

4 (2) The process to establish affiliate and other partnership
5 relationships to establish and maintain an advanced computing
6 infrastructure.

7 (3) A framework to determine the parameters for use of
8 CalCompute, including, but not limited to, a process for deciding
9 which projects will be supported by CalCompute and what
10 resources and services will be provided to projects.

11 (4) A process for evaluating appropriate uses of the public cloud
12 resources and their potential downstream impact, including
13 mitigating downstream harms in deployment.

14 (5) An evaluation of the landscape of existing computing
15 capability, resources, data, and human expertise in California for
16 the purposes of responding quickly to a security, health, or natural
17 disaster emergency.

18 (6) An analysis of the state's investment in the training and
19 development of the technology workforce, including through
20 degree programs at the University of California, the California
21 State University, and the California Community Colleges.

22 (7) A process for evaluating the potential impact of CalCompute
23 on retaining technology professionals in the public workforce.

24 (d) The Department of Technology shall submit, pursuant to
25 Section 9795, an annual report to the Legislature from the
26 commissioned consultants to ensure progress in meeting the
27 objectives listed above.

28 (e) The Department of Technology may receive private
29 donations, grants, and local funds, in addition to allocated funding
30 in the annual budget, to effectuate this section.

31 (f) This section shall become operative only upon an
32 appropriation in a budget act for the purposes of this section.

33 SEC. 6. The provisions of this act are severable. If any
34 provision of this act or its application is held invalid, that invalidity
35 shall not affect other provisions or applications that can be given
36 effect without the invalid provision or application.

37 SEC. 7. This act shall be liberally construed to effectuate its
38 purposes.

39 SEC. 8. The duties and obligations imposed by this act are
40 cumulative with any other duties or obligations imposed under

1 other law and shall not be construed to relieve any party from any
2 duties or obligations imposed under other law.

3 SEC. 9. No reimbursement is required by this act pursuant to
4 Section 6 of Article XIII B of the California Constitution because
5 the only costs that may be incurred by a local agency or school
6 district will be incurred because this act creates a new crime or
7 infraction, eliminates a crime or infraction, or changes the penalty
8 for a crime or infraction, within the meaning of Section 17556 of
9 the Government Code, or changes the definition of a crime within
10 the meaning of Section 6 of Article XIII B of the California
11 Constitution.

O

Introduced by Senator Dodd

February 14, 2024

An act relating to public postsecondary education.

LEGISLATIVE COUNSEL'S DIGEST

SB 1166, as introduced, Dodd. Public postsecondary education: prevention of discrimination.

Existing law establishes the California Community Colleges under the administration of the Board of Governors of the California Community Colleges, the California State University under the administration of the Trustees of the California State University, and the University of California under the administration of the Regents of the University of California as the 3 segments of public postsecondary education in the state. Existing law makes the governing boards of institutions of higher education responsible for ensuring and maintaining multicultural learning environments free from all forms of discrimination and harassment.

This bill would declare the intent of the Legislature to enact subsequent legislation that would establish reporting requirements on public postsecondary educational institutions relating to the prevention of discrimination.

Vote: majority. Appropriation: no. Fiscal committee: no. State-mandated local program: no.

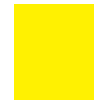
The people of the State of California do enact as follows:

- 1 SECTION 1. It is the intent of the Legislature to enact
- 2 subsequent legislation that would establish reporting requirements

- 1 on public postsecondary educational institutions relating to the
- 2 prevention of discrimination.

O

(DRAFT) Solano County 2024 Legislative Committee Calendar - approved by BOS (date TBD)



Release Legislative Committee Agenda

Proposed Legislative Committee Meeting

Legislative Report to Board of Supervisors

Annual / Legislative Conference Event

Solano County Recognized Holiday

State of California Recognized Holiday

JANUARY						
S	M	T	W	Th	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

January 1, Statutes take effect
January 3, Legislature reconvenes
January 10, Budget deadline for Governor
January 15, Martin Luther King Jr. Holiday
January 19, Last day for any committee to hear/report to the floor bills introduced in that house in odd-numbered years. Last day to submit bill requests to the Office of the Leg. Counsel
January 31, Last day for each house to pass bills introduced into that house in odd-numbered year

FEBRUARY						
S	M	T	W	Th	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29		

February 10-13, NACo Leg. Conference (Wash. D.C.)
February 12, President Lincoln's birthday
February 16, Last day for bills to be introduced
February 19, President Washington's Day
February 29, Legislative Committee Agenda released

MARCH						
S	M	T	W	Th	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

March 4, Legislative Committee meeting
March 12, Legislative Report to Board of Supes.
March 21, Spring recess begins upon adjournment
March 29, Cesar Chavez Day observed

APRIL						
S	M	T	W	Th	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

April 1, Legislature reconvenes from Spring recess
April 11, Legislative Committee Agenda released
April 15, Legislative Committee meeting
April 17-19, CSAC Legislative Conference (Sacramento)
April 23, Legislative Report to Board of Supes.
April 26, Last day for policy committees to hear and report to fiscal committees; fiscal bills introduced in their house



Legislative Committee meetings start at 1:30 p.m. PST and Board meetings start at 9 a.m. PST (unless otherwise stated on the agenda packet)

(DRAFT) Solano County 2024 Legislative Committee Calendar - approved by BOS (date TBD)



Release Legislative Committee Agenda

Proposed Legislative Committee Meeting

Legislative Report to Board of Supervisors

Annual / Legislative Conference Event

Solano County Recognized Holiday

State of California Recognized Holiday

MAY						
S	M	T	W	Th	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

May 3, Last day for policy committees to hear and report to the Floor non-fiscal bills introduced into their house

May 10, Last day for policy committees to meet prior to May 28, 2024

May 17, Last day for fiscal committees to hear and report to the Floor bills introduced into their houses; last day for fiscal comms to meet prior to June 5

May 20 – 24, Floor session only. No committees other than conference or rules committees may meet for any purpose.

May 24, Last day for each house to pass bills introduced in that house

May 27, Memorial Day holiday

May 28, Committee meetings may resume

May 30, Legislative Committee Agenda released

JUNE						
S	M	T	W	Th	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

June 3, Legislative Committee meeting

June 11, Legislative Report to Board of Supes.

June 13, Legislative Committee Agenda released

June 15, Budget must be passed by midnight

June 17, Legislative Committee meeting

June 19, Juneteenth holiday

June 25, Legislative Report to Board of Supes.

June 27, Last day for legislative measure to qualify for the Nov. 5, 2024 General Election ballot

JULY						
S	M	T	W	Th	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

July 3, Last day for policy committees to meet and report bills. Summer recess begins upon adjournment provided Budget Bill has passed

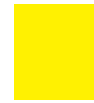
July 4, Independence Day

July 12 – 15, NACo Annual Conference (Hillsborough County, Florida)

Legislative Committee meetings start at 1:30 p.m. PST and Board meetings start at 9 a.m. PST (unless otherwise stated on the agenda packet)



(DRAFT) Solano County 2024 Legislative Committee Calendar - approved by BOS (date TBD)



Release Legislative Committee Agenda

Proposed Legislative Committee Meeting

Legislative Report to Board of Supervisors

Annual / Legislative Conference Event

Solano County Recognized Holiday

State of California Recognized Holiday

AUGUST						
S	M	T	W	Th	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

August 5, Legislature reconvenes from Summer Recess

August 16, Last day for fiscal committees to meet and report bills

August 19-31, Floor session only. No committees, except conference and Rules committees may meet

August 23, Last day to amend on the floor

August 31, Last day for each house to pass bills. Final recess begins upon adjournment

SEPTEMBER						
S	M	T	W	Th	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

September 2, Labor Day holiday

September 27, Proposed 2025 Legislative Platform Changes due to CAO's Office

September 30, Last day for Governor to sign or veto bills passed by the Legislature before Sept. 1 and in the Governor's possession on or after Sept. 1

OCTOBER						
S	M	T	W	Th	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

October 2, Bills enacted on or before this date take effect January 1, 2025

October 14, Indigenous Peoples' Day holiday

October 17, Legislative Committee Agenda released

October 21, Legislative Committee's review of 2025 Legislative Platforms / edits

Legislative Committee meetings start at 1:30 p.m. PST and Board meetings start at 9 a.m. PST (unless otherwise stated on the agenda packet)



(DRAFT) Solano County 2024 Legislative Committee Calendar - approved by BOS (date TBD)



Release Legislative Committee Agenda

Proposed Legislative Committee Meeting

Legislative Report to Board of Supervisors

Annual / Legislative Conference Event

Solano County Recognized Holiday

State of California Recognized Holiday

NOVEMBER						
S	M	T	W	Th	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

November 5, Board of Supervisors first review of 2025 Legislative Platforms (*a second review will be scheduled for a later date if changes are necessary*)
November 5, General Election
November 11, Veteran’s Day holiday
November 18-22, CSAC Annual Conference (Los Angeles County)
November 28-29, Thanksgiving holiday
November 30, Adjournment *Sine Die* at midnight

DECEMBER						
S	M	T	W	Th	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

December 2, Noon convening of 2025-26 Session
December 24, Half-day pre-Christmas closure
December 25, Christmas Day holiday observed
December 31, New Year’s Eve half-day closure
December 31, Last Day to distribute 2025 Legislative Platforms to Solano Delegation

January 1, 2025, Statutes take effect

