Date of Hearing: August 20, 2025

ASSEMBLY COMMITTEE ON APPROPRIATIONS
Buffy Wicks, Chair
SB 53 (Wiener) – As Amended July 17, 2025

Policy Committee:	Judiciary	Vote:	12 - 0
	Privacy and Consumer Protection		10 - 0

Urgency: No State Mandated Local Program: No Reimbursable: No

SUMMARY:

This bill imposes reporting and auditing requirements on large developers of foundation artificial intelligence (AI) models ("foundation models'), requires the Government Operations Agency (GovOps) to develop a framework for a public cloud computing cluster, and enacts whistleblower protections related to activities of large developers.

Specifically, among other provisions, this bill:

1) Requires a large developer to implement, publish, and update a safety and security protocol that includes, among other specified elements, how the developer assesses catastrophic risks from a foundation model, the actions the developer will take if a risk threshold is attained by a model, the role of third-party assessment of catastrophic risk in the developer's protocol, and the developer's cybersecurity practices.

2) Requires a large developer to publish a transparency report before or at the same time as the developer deploys a new foundation model. The report must include specified information about any risk assessment performed on the new model and the developer's reasoning behind deploying the new model.

3) Requires a large developer to publish any assessment of catastrophic risk or dangerous capabilities resulting from internal use of its foundation models, according to the schedule the developer specifies in its safety and security protocol.

4) Prohibits a large developer from making a materially false or misleading statement about catastrophic risk from its foundation models, its management of catastrophic risk, or its implementation of or compliance with its safety and security protocol.

5) Requires the Attorney General (AG) to establish a mechanism through which a large developer or a member of the public may report a critical safety incident, and requires critical safety incident reporting by a large developer, as specified.

6) Requires the AG to review critical safety incidents submitted by a large developer and permits the AG to review critical safety incidents submitted by members of the public.

7) Requires the AG, beginning January 1, 2027, to produce an annual report of anonymized and aggregated information from critical safety incident reports, whistleblower reports, and summaries of auditor's reports. The report must be distributed to the Governor's Office and the Legislature.

8) Requires a large developer, beginning January 1, 2030, and at least annually thereafter, to retain an independent third party auditor to produce a report assessing whether the developer has substantially complied with its safety and security protocol, as specified, and requires an auditor to transmit to the AG a high-level summary of the audit report within 30 days after completing an audit.

9) Authorizes the AG to adopt regulations to update the definition of a "large developer" to ensure it accurately reflects technological developments, scientific literature, and widely accepted national and international standards and applies to well-resourced large developers at the frontier of AI development.

10) Authorizes the AG to bring a civil action to enforce a violation of the bill's provisions by a large developer and imposes civil penalties ranging from up to $10,000 to $10 million depending on the risk of harm associated with the violation and whether the violation was unknowing or knowing.

11) Authorizes the AG to bring a civil action to enforce a violation of the bill's provisions by an auditor and imposes a civil penalty of up to $10,000 for each violation.

12) Establishes within GovOps a consortium, as specified, to develop a framework for the creation of a public cloud computing cluster to be known as "CalCompute," and specifies elements that must be included in the framework, elements that must be included in CalCompute, and membership requirements for the consortium.

13) Requires GovOps, on or before January 1, 2027, to submit a report from the consortium to the Legislature with the framework for the creation and operation of CalCompute, as specified. Dissolves the consortium following submission of the report to the Legislature.

14) Requires the consortium to make reasonable efforts to ensure CalCompute is established within the University of California (UC) to the extent possible. If CalCompute is established within the UC, authorizes the UC to receive private donations for the purposes of implementing CalCompute.

15) Makes the bill's provisions pertaining to CalCompute operative only upon appropriation.

16) Establishes whistleblower protections for people who interact with large developers, including employees and contractors, among others, if they disclose information they have a reasonable cause to believe indicates the developer's activities pose a catastrophic risk or the developer has violated the bill's provisions, and requires a large developer to post notices and provide internal processes to facilitate information reporting.

FISCAL EFFECT:

1) Costs (General Fund) to the Department of Justice (DOJ), likely in the low millions of dollars annually, to establish reporting mechanisms, review critical incident reports, conduct investigations, publish reports, and enforce violations. DOJ anticipates costs of approximately $1.1 million in fiscal year 2025-26 and $2 million annually ongoing thereafter for eight staff positions (attorneys, analysts, IT specialists, and legal secretaries) in its Consumer Protection Section and external consultant costs. DOJ reports it is unable to absorb these costs and can implement this bill only with an appropriation of additional funding. DOJ may also incur enforcement costs for violations of the bill's whistleblower protections; the bill does not clearly specify the entity responsible for this enforcement but permits an employee making a whistleblower report to use an existing DOJ whistleblower hotline.

2) Costs (General Fund) to GovOps to establish and operate the CalCompute consortium until January 1, 2027, possibly in the high hundreds of thousands of dollars to low millions of dollars. GovOps estimates total costs of $2.5 million for expert contractors, infrastructure planning, and staffing to manage the project, conduct research, and develop the required report. GovOps was not able to provide a breakdown of these costs but anticipates the workload would be handled by contract workers due to the short timeframe in the bill. Members of the consortium are not entitled to compensation but are entitled to reimbursement for necessary expenses incurred in performing their duties; these costs were not included in GovOps' fiscal estimate but may be in the thousands to low tens of thousands of dollars depending on the activities of the consortium.

3) Possible cost pressures (General Fund) of an unknown but potentially significant amount to the UC to operate CalCompute, should it be established within the UC. State costs may be offset to some extent by private donations, which the bill authorizes the UC to receive to implement CalCompute.

4) Costs (General Fund, Labor and Enforcement Compliance Fund) of an unknown but potentially significant amount to the Labor Commissioner to enforce violations of the bill's whistleblower provisions. Actual costs will depend on the number of violations, the number of actions pursued, and the amount of workload associated with each action.

5) Cost pressures (Trial Court Trust Fund, General Fund) to the courts to adjudicate enforcement actions and whistleblower cases. Actual costs will depend on the number of violations, the number of actions filed, and the amount of court time needed to resolve each case. It generally costs approximately $1,000 to operate a courtroom for one hour. Although courts are not funded on the basis of workload, increased pressure on the Trial Court Trust Fund may create a demand for increased funding for courts from the General Fund. The fiscal year 2025-26 state budget provides $82 million ongoing General Fund to the Trial Court Trust Fund for court operations.

COMMENTS:

As the development of AI models has progressed, scholars, policymakers, philosophers, and others have raised concern about the lack of regulation for the most powerful emerging AI models. As discussed thoroughly in the policy committee analyses of this bill, many people

inside and outside the industry have encouraged governments to put an anticipatory regulatory framework in place now, despite the considerable uncertainty about the future of AI modeling, to mitigate the risk of future harm resulting from AI models.

Last year, the Legislature passed SB 1047 (Wiener), which, among other provisions, would have established a state board to regulate frontier AI models and imposed testing and reporting requirements on developers before they could train, use, or make publicly available a covered frontier model. SB 1047 also contained some elements that were similar to this bill, including whistleblower protections and a consortium to create a public computing cluster. Governor Newsom vetoed SB 1047. In a lengthy veto message, the Governor cited the fact that the bill would have rigorously regulated only the most expensive and large-scale models, without taking into account the particular features and applications of each model:

> While well-intentioned, SB 1047 does not take into account whether an AI system is deployed in high-risk environments, involves critical decision-making or the use of sensitive data. Instead, the bill applies stringent standards to even the most basic functions - so long as a large system deploys it. I do not believe this is the best approach to protecting the public from real threats posed by the technology.

On the same day he vetoed SB 1047, Governor Newsom announced he had convened a working group of experts to "help California develop workable guardrails" for generative AI and frontier AI models. In June 2025, the working group released its final report on frontier AI policy. The report includes discussion of and recommendations related to many aspects of AI development and regulation, including transparency into the activities of AI companies, how adverse events should be reported to regulators and the public, and factors to consider when tailoring the scope of state regulations on developers and deployers of AI technology.

This bill integrates recommendations of the working group, modified elements of SB 1047, and input from other stakeholders to create a regulatory regime for foundation AI models. According to the author, the result is a more balanced approach that "allows California to continue to maintain its leadership in the AI development ecosystem and to demonstrate that safety does not stifle success." The bill is sponsored by Encode Justice, Secure AI Project, and Economic Security California Action, and is supported by groups that favor greater regulation of the AI industry. The bill is opposed by business and industry representatives, including the California Chamber of Commerce, Chamber of Progress, and TechNet.

Analysis Prepared by: Annika Carlson / APPR. / (916) 319-2081