SB 1047 Section-By-Section

Section 1. Short Title.

Names the bill the Safe and Secure Innovation for Frontier Artificial Intelligence Models Act.

Section 2. Sense of the legislature.

Declares that California is leading the world in Artificial Intelligence (AI) and that California’s government has an essential role to play in ensuring Californians receive the benefits of this technology while being protected from the most severe risks.

Section 3. Safety of frontier AI models.

Section 22602. Definitions. Selected definitions:

“Covered models” are the limited group of the frontier AI models subject to the act. To qualify, an AI model must be trained using greater than $10^{26}$ operations, OR an amount of computing power such that it could reasonably be expected to have similar performance to a model trained with $10^{26}$ operations in 2024. AI models that do not qualify as covered models are not subject to the act.

“Hazardous capability” is the term used to describe the severe risks of AI that the act seeks to prevent. The term covers the capability of a covered model to enable any of the following critical harms in a way that would be significantly more difficult to cause without access to a covered model:

1. The creation or use of a chemical, biological, radiological, or nuclear weapon in a manner that results in mass casualties.
2. At least $500$ million of damage through cyberattacks on critical infrastructure.
3. At least $500$ million of damage by an artificial intelligence model that autonomously engages in conduct that would be criminal if undertaken by a human.
4. Other equally severe threats to public safety and security.

Hazardous capabilities include capabilities that would only manifest if a model is fine-tuned.

“Limited duty exemption” means an exemption that is available when a developer can reasonably exclude the possibility that a covered model has or may come close to having a hazardous capability. In short, the act is focused on covered models with hazardous capabilities. If a covered model does not come close to having such hazardous
capabilities the developer of a covered model would have only limited obligations under the act. However, if a covered model does have a hazardous capability, the developer would need to put in place safeguards to prevent abuse of such a hazardous capability.

- A developer is not required to have a limited duty exemption. If a covered model does not qualify for that exemption, the developer can comply with the act by putting in place various safeguards to prevent abuse of any hazardous capability.
- Developers make their own assessments of whether they qualify for a limited duty exemption and provide an appropriate exemption to the Frontier Model Division. Developers may secure a limited duty exemption on two occasions: first, prior to training (22603(a)), and second, after completion of training (22603(c)).

“Covered guidance” means guidance relevant to the management of safety risks associated with AI models with hazardous capabilities issued by the Frontier Model Division and the National Institute of Standards and Technology (within the U.S. Department of Commerce); or industry best practices.

“Frontier Model Division” is a new division in the California Department of Technology, created in Section 4.

Section 22603. Safety requirements.

22603(a) If a covered model has lower performance under relevant benchmarks and has lower general capability than another covered model that lacks hazardous capability, the model is eligible for a limited duty exemption that relieves the developer from most of the requirements of the act. A developer that claims such an exemption shall submit a certification to the Frontier Model Division. If a developer makes a good faith error in this determination, it has 30 days after training the model to correct it.

22603(b) If a developer does not claim a limited duty exemption at the above step, then the developer must do all of the following prior and during training:

1. Implement cybersecurity controls to prevent model theft.
2. Implement the capability to fully shut down the model.
3. Implement covered guidance.
4. Develop a written safety and security protocol for submission to the Frontier Model Division that describes how the model will be prevented from possessing or exercising hazardous capabilities and how the model will be tested for hazardous capabilities. The protocol must be implemented as written and senior personnel must be designated to ensure compliance.
5. Refrain from initiating training of a covered model if there remains unreasonable risk that hazardous capabilities will be exercised to cause a critical harm.

22603(c) After a covered model that is not the subject of a limited duty exemption completes training, the developer must perform capability testing to determine whether it
lacks hazardous capabilities and therefore can be subject to a limited duty exemption. The developer must submit its assessment of whether a limited duty exemption applies and the testing results to the Frontier Model Division.

22603(d) If after capability testing, a model continues to have or be close to having a hazardous capability, the developer must:
1. Implement reasonable safeguards to prevent individuals from using hazardous capabilities or creating derivative models with hazardous capabilities.
2. Create methods to attribute model actions and resulting harms to the model and its user.
3. Refrain from releasing a covered model if there is still an unreasonable risk that a hazardous capability will be exercised.
4. Implement any other reasonably necessary measures to prevent the exercise of hazardous capabilities.

22603(e) Developers must periodically reevaluate all of the safeguards put in place as described above.

22603(f) Developers of a model that is not subject to a limited duty exemption must annually certify compliance with the requirements in Section 22603 to the Frontier Model Division under penalty of perjury and submit information on any steps and evaluations required above.

22603(g) Developers must report AI safety incidents to the Frontier Model Division within 72 hours of learning of them.

22603(h) Reliance on an unreasonable limited duty exemption does not relieve a developer of its obligations. An exemption is unreasonable if it does not take into account reasonably foreseeable risks of harm or weaknesses in capability testing.

Section 22604. Know-your-customer rules.

To ensure greater accountability for the development of covered models, operators of computing clusters must implement know-your-customer rules for all customers using enough computing resources to train a covered model and assess whether customers intend to deploy a covered model. The developer must provide records of actions taken under this section to the Frontier Model Division upon request. The developer does not need to provide the customer records themselves to the Frontier Model Division.

Section 22605. Fair price schedules.

Developers providing commercial access to covered models must provide a transparent, uniform, publicly available price schedule. Computing clusters must also do this but can
provide discounted or preferential access to public entities, academic institutions, or for noncommercial research purposes.

Section 22606. Authorities of the Attorney General.

If the Attorney General finds that a person is violating this chapter, the Attorney General may bring a civil action. In response to harm or an imminent risk to public safety, courts can order relief including preventive relief and deletion of model weights. Civil actions can also result in punitive damages and an order for the full shutdown of the covered model, as well as civil penalties for violations. To give developers and computing cluster operators adequate time to come into compliance with the act, monetary damages cannot be awarded for violations before July 1, 2025, and courts cannot order model deletion, model shutdown (unless there is an imminent threat to public safety), or civil penalties for violations before January 1, 2026.

Section 22607. Whistleblower protections.

To ensure that critical information is passed along to the government agencies that need to know about it, employees of frontier AI model developers are protected by broad whistleblower provisions when they report violations of this act. Developers must also provide reasonable internal processes through which employees can anonymously provide internal reports of non-compliance with the requirements in Section 22603.

Section 22608. Cumulative duties.

The duties under this law are cumulative with duties imposed by other laws.

Section 4. Frontier Model Division.

Establishes the Frontier Model Division within the Department of Technology, which has the following duties:
1. Reviewing certification reports from developers.
2. Advising the Attorney General on potential violations.
3. Issuing guidance, including standards for auditors to run an optional accreditation process.
5. Issuing guidance on safety events that are likely to constitute a state of emergency under California law.
6. Appointing an advisory committee to advise the Governor on when it may be necessary to proclaim an AI-related state of emergency.
7. Appointing an advisory committee for open-source AI to issue guidelines for open-source models without hazardous capabilities and advise the Frontier Model
Division on potential incentives for open-source non-covered models and policies impacting open-source.

8. Levying fees from developers to fund the Frontier Model Division.

9. Developing proposed model jury instructions for the enforcement of the act.

10. By July 1st, 2026, issuing guidance regarding technical thresholds relevant for determining whether an AI model is covered and/or subject to a limited duty exemption.

11. Updating guidance at least every 24 months.

Section 5. CalCompute.

11547.7.

Directs the Department of Technology to establish the CalCompute public computing resource.

A. Grants authority to the Department of Technology to commission consultants to establish CalCompute, which must be fully owned and hosted by the state.

B. CalCompute consultants can include national labs, universities, and the private sector.

C. The Department must commission consultants to create a plan for CalCompute, including which projects will be prioritized, mitigation of downstream harms, and evaluation of the current cloud landscape.

D. Requires the Department of Technology to submit an annual report to the legislature on progress establishing CalCompute.

E. CalCompute may receive private donations, grants, and local funds.

F. This section becomes operative upon appropriation.

Section 6. Severability.

The provisions of the act are severable.

Section 7. Construction

The act shall be liberally construed.

Section 8. Reimbursement.

Disclaims reimbursements pursuant to Section 6 of Article XIII B of the California Constitution.