August 7, 2025

The Honorable Buffy Wicks, Chair
Assembly Appropriations Committee
1021 O Street, Room 8220
Sacramento, CA 95814

RE: SB 53 (Wiener) – artificial intelligence models: large developers. – SUPPORT

Dear Chair Wicks,

On behalf of the organizations signed below, we write to you today in support of SB 53 (Wiener), as amended on July 17th, 2025. This measure would establish a consortium at the Government Operations Agency to develop recommendations around the development of CalCompute, a public cloud computing cluster. It would also create transparency requirements for the safety and security requirements of the largest developers of AI foundation models, would require the reporting of serious incidents to the Attorney General, and would establish important whistleblower protections for those who report critical risks of AI foundation models. Starting in 2030, AI model developers subject to this measure would be required to contract with third party auditors to ensure they are complying with their Safety and Security Protocol.

Overall, the cost of this measure is greatly outweighed by the benefits of avoiding catastrophic harm. Of note, the CalCompute provisions are contingent upon appropriation, so do not cause additional state cost. The provisions that will generate some state costs are related to incident reporting, potential future regulatory action by the Attorney General to revise the scope of covered entities, and any enforcement pursued by the Attorney General. If enforcement is pursued and results in a civil penalty outlined by the bill, the costs of this measure would be more than recovered by that enforcement action.

The California Report on Frontier AI Policy, while it does not endorse any specific legislation, forms the foundation for SB 53. Established by Governor Newsom in 2024 and led by Dr. Fei-Fei Li, Dr. Jennifer Tour Chayes and Mariano-Florentino Cuéllar, the report is anchored on the notion of "trust but verify" and calls for more transparency into the safety practices of AI companies, adverse event reporting requirements, and whistleblower protections. SB 53 implements these principles.

Large AI developers are developing increasingly advanced AI systems. We are excited about the potential for these systems to drive improvements in education, science, provisioning of public

services, and more. At the same time, large AI developers themselves warn that their **AI systems could pose serious risks,** which they have voluntarily committed to addressing. The Report stated that "some risks have unclear but growing evidence...AI-enabled hacking or biological attacks, and loss of control" – the risks that SB 53 aims to address and gather more evidence about. Advanced AI is currently mostly unregulated, and these risks are currently being managed by companies themselves without any requirement that they inform the public about their risk management practices or report serious incidents. SB 53 addresses this much needed gap by implementing four key recommendations from the report.

First, the Report argued that "transparency into the risks associated with foundation models, what mitigations are implemented to address risks, and how the two interrelate is the foundation for understanding how model developers manage risk." SB 53 implements this recommendation as a requirement for large AI developers to **write, publish, and follow safety and security protocols** to manage the most severe risks. This is in line with voluntary commitments that companies have already made. Rather than prescribe specific technical standards that companies must take, the bill simply requires companies to be transparent about the approaches they are using. Some of the specific required elements of safety protocols, such as a requirement to manage risks related to internal use of AI models and cybersecurity policies, directly mirror recommendations in the Report. Others mirror components of the Stanford Foundation Model Transparency Index, which is cited prominently in the Report.

Second, the Report stated that "transparency into pre-deployment assessments of capabilities and risks, spanning both developer-conducted and externally conducted evaluations, is vital given that these evaluations are early indicators of how models may affect society and may be interpreted (potentially undesirably) as safety assurances." SB 53 accomplishes this with a **requirement that large developers publish transparency reports that include the results of their pre-deployment assessments of catastrophic risk**. The Report also argues that "transparency into the safety cases used to assess risk provides clarity into how developers justify decisions around model safety," which forms the basis for 22757.12(c)(3).

Third, the Report concluded that "an **adverse event reporting system** that combines mandatory developer reporting with voluntary user reporting maximally grows the evidence base." SB 53 takes exactly this approach by establishing a tightly defined set of critical safety incidents that AI developers are required to report to the Attorney General. It would also allow members of the public to optionally submit reports.

Finally, the Report recommends strengthening **whistleblower protections**, pointing out that "actions that may clearly pose a risk and violate company policies...may not violate any existing laws. Therefore, policymakers may consider protections that cover a broader range of activities, which may draw upon notions of 'good faith' reporting on risks found in other domains such as cybersecurity." This recommendation is mirrored in SB 53, which allows employees to report evidence of catastrophic risks as well as violations of SB 53 itself to government authorities with legal protections against retaliation.

SB 53 only applies to the largest AI developers – those training models with more than 10^26 floating point operations (FLOPs). These are companies spending hundreds of millions or billions of dollars to train the most advanced AI models. It would impose no burden on smaller companies and the requirements it imposes on large companies are minimal compared to what companies are already voluntarily doing. The Report argues that "policymakers should ensure that mechanisms are in place to adapt thresholds over time—not only by updating specific threshold values but also by revising or replacing metrics if needed." It also suggests specific criteria that thresholds should be evaluated for. Following this recommendation, SB 53 allows the Attorney General to update the definition of "large developer" through regulation while considering the same factors described in the report. Regardless of any update, the Attorney General must only include "well-resourced large developers at the frontier of artificial intelligence development" in the scoping of the bill. If legislation is needed to cover other developers, the Attorney General is instructed to write a report to the Legislature requesting it.

Finally, **SB 53 would also set in motion CalCompute**, a public cloud computing cluster for use by academics and startups in California. Computational resources are essential for AI research and CalCompute would make those resources more accessible to California's top universities and startups, helping to catalyze additional research into beneficial applications of AI and supporting, in particular, smaller startups for a healthier innovation ecosystem. This mirrors a similar computing cluster that is already being established in New York state. We support this groundbreaking effort, which would advance and democratize AI research in California.

SB 53 thoughtfully implements the recommendations of the Report by combining a low-burden transparency and reporting regime with a public compute cluster that will broaden access for AI researchers and startups in California. This is a commonsense approach that will strengthen the AI ecosystem, benefiting both companies and the public interest.

For all these reasons, we respectfully urge your support of this important measure.

Sincerely,
Thomas Woodside, Secure AI Project (co-sponsor)
Nathan Calvin, Encode AI (co-sponsor)
Teri Olle, Economic Security California Action (co-sponsor)

Daniel Kokotajlo, AI Futures Project
Buck Shlegeris, Redwood Research
Matt Larson, Secure AI Future
Esben Kran, Apart Research
Bhaskar Bhatt, AI Policy Tracker
Emerson Spartz, Nonlinear
Connor Flexman, EarningsStream LLC
Andreas Stuhlmüller, Elicit
Zach Stein-Perlman, AI Lab Watch
Tyler Johnston, The Midas Project

Jacob Eliosoff, Trevi Digital Assets Fund
Michael Andregg, Eon Systems
Oliver Edholm, Depict.ai
Nick Fitz, Momentum
Constance Li, AI for Animals
Barbara Patch, All Girls Allowed
Delphine Halgand-Mishra, The Signals Network
Sacha Haworth, Tech Oversight California
Keith Dunn, District Council of Iron Workers
David Manheim, Association for Long Term Existence and Resilience (ALTER)
Saheb Gulati, Center for Youth and AI
Otto Barten, Existential Risk Observatory
Anshi Bhatt, Frontlines Foundation
Nadav Brandes, Brandes Lab at NYU
Mikey Hothi, Common Sense Media
Ivan Fernandez, California Federation of Labor Unions, AFL-CIO
Darius Emrani, Scorecard
Evelina Ayrapetyan, Center for AI and Digital Policy
Jai Jaisimha, Transparency Coalition
Alexandra Tsalidis, Future of Life Institute
Mark Nitzberg, Center for Human Compatible AI

cc: The Honorable Kate Sanchez, Vice Chair, Assembly Appropriations Committee
Members, Assembly Appropriations Committee