Why SB 53 Would be Inadequate as a Federal Standard

California's SB 53 is a good first step for transparency, but it would be woefully inadequate as a federal framework. SB 53 lacks a verification mechanism to ensure companies are keeping commitments, standards to ensure those commitments are up to par, flexibility to evolve the law to changing technical circumstances, and any emergency response mechanism. **Even if a company identifies a substantial catastrophic risk from a currently deployed AI system, SB 53 contains no requirement to mitigate that risk in any way.** Without these elements, SB 53 falls far short of what is needed to protect the public from serious catastrophic risks.

Why guarding against catastrophic risks is important

AI developers have themselves repeatedly stated that their most advanced AI systems may pose catastrophic risks, and they have voluntarily committed to addressing those risks. The California Report on Frontier AI Policy, commissioned by Governor Gavin Newsom and led by Dr. Fei-Fei Li, Dr. Jennifer Tour Chayes and Dr. Tino Cuéllar, said that: "Evidence that foundation models contribute to both chemical, biological, radiological, and nuclear (CBRN) weapons risks for novices and loss of control concerns has grown, even since the release of the draft of this report in March 2025." Just this year, multiple companies have stated their frontier models pose updated risks of enabling biological threats, and multiple companies have discovered their models being used for offensive cyberattacks.

SB 53 provides transparency, but mere transparency is insufficient

California recently enacted SB 53, which provides a transparency framework for the largest developers of the most advanced AI models. It requires those large developers to:

- Publish frameworks for how they assess and mitigate catastrophic risks, defined as CBRN attacks, autonomous criminal activity such as cyberattacks, and loss of control.
- Publish the results of catastrophic risk assessments they conduct.
- Report major incidents and summaries assessments of risks of internal use from their AI models privately to government agencies.
- Protect whistleblowers.

It also holds AI developers legally accountable to their own commitments. SB 53 is a first step towards more transparency, allowing the public and independent experts to critique company practices. But it falls short in many ways that make it inapt as a federal standard. Even Governor Newsom said that the bill "does a little, not enough." He added: "I'm just being candid."

SB 53 lacks verification

Although companies are legally held to their own commitments under SB 53, the law provides no systematic way to verify compliance. Compliance will have to be enforced through media reports, whistleblower tips, and suspicions of the California Attorney General.

The California Report on Frontier AI Policy said that "Transparency alone is insufficient; as the tobacco case shows, companies can distort public understanding despite available evidence. Independent verification mechanisms are necessary to validate industry claims and ensure that evidence is accurately represented…"

Without a robust third party verification requirement, SB 53 risks being enforced only in fairly egregious cases. This is why legislators from both parties in states like Illinois and Michigan have introduced bills that include third party auditing requirements.

SB 53 lacks standards

Even if company commitments could be verified, SB 53 does not require any level of sufficiency to those commitments. Nothing in SB 53 prevents a big AI company from saying in effect, "we do essentially nothing to assess or mitigate these risks because we don't think they are important."And if a company ever decides to discard a commitment, even at the expense of public safety, it can swiftly do so simply by publishing an updated policy.

That's why the RAISE Act, a bill passed with bipartisan support in New York state, requires companies to have reasonable safety protocols, cybersecurity protections, and safeguards and avoid releasing models that pose unreasonable catastrophic risks. This would provide recourse against companies that fail to protect the public.

In a federal law, agencies should also have the authority to initiate formal standard setting processes and hold companies to those standards. Such standards could identify industry best practices emerging from industry commitments, including minimum safety measures.

SB 53 lacks updateability

The text of SB 53 itself acknowledges that it may become out of date over time, and the law tasks an agency to deliver an annual report to the legislature recommending changes to key definitions. Many state legislatures, including California, are highly active and pass hundreds of substantive standalone bills per year, making it likely that they can update the law in the future if needed. But updating a federal law can be extremely difficult, taking years even when there is a general agreement on the need for a change.

Any federal law would need to provide an agency with authority to adjust which models and developers are covered and which safety framework elements and incidents must be reported. Otherwise, Congress could lock in a standard that cannot keep up with an evolving technology.

SB 53 lacks emergency response

In a field as fast-moving as AI, slow-moving standard setting processes, verification, and transparency may be insufficient to protect the public from unexpected dangers. If the federal government learns, perhaps through transparency and verification procedures, that a catastrophic risk is occurring or imminently about to occur, it will need to take rapid action. Any federal law would need to empower federal experts in catastrophic risks from AI to plan for and respond to such an outcome, including with appropriate legal authorities for their response.