California Lawmakers Pass Landmark AI Transparency Law for Frontier Models: How SB 53 Differs from Last Year's Failed Attempt

Insights
9.15.25

The California legislature just passed the nation's first comprehensive attempt to require safety and transparency reporting for the most powerful AI systems – and now all eyes turn to the Governor's office to see if he'll approve it. Lawmakers approved SB 53, also known as the Transparency in Frontier Artificial Intelligence Act, by a 29-8 vote in the Senate and an 45-7 vote in the Assembly late Friday night as the legislative session wrapped up. The move comes one year after Governor Newsom vetoed a broader AI safety bill (SB 1047) that drew criticism for imposing heavy-handed mandates. SB 53 represents a strategic shift, but one that businesses and employers will still need to pay close attention to. What do tech companies – and employers that use AI – need to know about this landmark new law in advance of Governor Newsom's October 12 deadline to veto or sign?

From Veto to Victory: What Changed Since SB 1047

Last year's SB 1047 sailed through the legislature but was blocked at the Governor's desk over fears it would stifle California's AI competitiveness. That bill:

- Required **kill switches** and shutdown mechanisms for frontier models.
- Mandated **extensive pre-launch and ongoing testing**.
- Imposed **strict liability provisions** on developers.
- Set an aggressive **72-hour timeline** for incident reporting.

By contrast, SB 53 takes a transparency-first approach:

- **No kill switch** requirement.
- No rigid testing regime – instead, developers must **publish "frontier AI frameworks"** explaining how they assess and mitigate risks.
- **Critical safety incident reporting** is required, but developers have **15 days** to do so (24 hours if imminent harm).
- Focuses narrowly on **"large frontier developers"** (>$500M in annual revenue, training models at ≥10^26 FLOPs), sparing smaller companies from immediate obligations.

The bill was drafted in line with the Governor's California AI Policy Blueprint, which emphasized evidence-building and standardized disclosures over prescriptive controls.

3 Core Requirements for Frontier Developers

What do affected tech businesses need to know about this first-of-its-kind new law? SB 53's obligations fall into three main buckets:

1. Frontier AI Frameworks

Developers must publish and update annual frameworks describing risk thresholds, mitigations, third-party assessments, governance practices, and cybersecurity measures for protecting model weights.

2. Transparency Reports

Before releasing a covered model, companies must publish reports detailing release date, languages, modalities, intended uses, restrictions, and summaries of catastrophic risk assessments.

3. Critical Safety Incident Reporting

Developers must notify the Office of Emergency Services (OES) within 15 days of a qualifying incident (such as loss of control or malicious misuse), or within 24 hours if the risk is imminent. OES will issue anonymized annual summaries beginning in 2027.

Whistleblower Protections and CalCompute

There are two additional provisions for tech companies to be aware of:

- **Whistleblower Protections**: Employees responsible for assessing or managing AI risks are shielded from retaliation if they report safety concerns to regulators or internally. Large developers must also maintain anonymous reporting channels.
- **CalCompute**: The bill creates a framework for a public cloud cluster, potentially housed at the University of California, to expand equitable access to compute resources. A governance and funding report is due in 2027.

Industry and Political Reactions

- **Anthropic endorsement**: The San Francisco-based AI company publicly backed SB 53 last week, calling it a *"trust-but-verify"* approach and praising its alignment with existing voluntary practices.

- **Policymakers**: Senator Scott Wiener, SB 53's sponsor, framed the bill as a landmark transparency measure that strengthens public trust without strangling innovation.
- **Observers**: Analysts note SB 53 is more likely to withstand gubernatorial scrutiny precisely because it trades prescriptive engineering mandates for standardized disclosure and accountability – and closely aligns with the blueprint he sought.

Effective Dates

- **Effective Date**: If enacted by the Governor, the law will apply effective January 1, 2026, to large frontier developers deploying new or substantially modified frontier models. That means frontier AI frameworks and transparency reports would need to be published *before or concurrently with deployment* of covered models after that date.
- **Critical safety incident reporting**: These reporting obligations (15 days, or 24 hours if imminent harm) would also kick in once the law is effective.
- **Staged reporting obligations**: By January 1, 2027:
  - The Office of Emergency Services (OES) must begin issuing annual anonymized reports of critical safety incidents.
  - The Department of Technology must begin reviewing definitions of "frontier model," "frontier developer," and "large frontier developer" each year.
  - The Government Operations Agency must submit its CalCompute governance framework report to the Legislature.
  - The Attorney General must begin publishing annual summaries of whistleblower reports.
- **Penalties**: Civil penalties (up to $1M per violation) are enforceable by the Attorney General immediately upon the law taking effect.

What This Means for Employers

Even though SB 53 directly regulates frontier developers, the ripple effects will reach employers who use, purchase, or contract for AI systems.

- **Contractual Flow-Downs**: Expect vendors to mirror SB 53 disclosures in system cards, model cards, and transparency statements.
- **Procurement Due Diligence**: Employers should begin asking vendors whether they comply with SB 53-style frameworks and incident reporting. You can add this to the list of questions you pose to your AI vendors.
- **Workforce Implications**: Whistleblower protections may influence employment practices, particularly around risk assessment and compliance roles.
- **Regulatory Roadmap**: California has signaled it will legislate in AI absent federal action. Employers should anticipate further sector-specific AI rules, especially in workplace and privacy

Employers should anticipate further sector-specific AI rules, especially in workplace and privacy contexts.

What's Next

- **All Eyes on Newsom**: The Governor has until October 12 to sign or veto the bill. He has yet to make a public comment about SB 53.
- **Rulemaking**: If the bill passes, OES will set up the incident reporting system and may recognize equivalent federal standards.
- **Annual Reports**: Starting in 2027, OES and the Attorney General would release anonymized summaries of incidents and employee reports if the bill becomes law.
- **CalCompute Development**: The governance consortium would deliver its design recommendations by January 1, 2027.
- **Potential Expansion**: The law acknowledges smaller developers may need regulation in the future if their models reach catastrophic-risk thresholds. 2026 could see even more AI legislation.

Conclusion

If you have any questions, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our AI, Data, and Analytics Practice Group, in any our California offices, or on our Government Relations team. Make sure you are subscribed to Fisher Phillips' Insight System to receive the latest developments straight to your inbox.

Related People

Benjamin M. Ebbink
Partner
916.210.0400
Email

Richard R. Meneghello
Chief Content Officer
503.205.8044
Email

Service Focus

AI, Data, and Analytics

Industry Focus

Tech

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills