



August 25, 2026

The Honorable Jerry McNerney
Senator, State of California
1021 O St, Suite 6640
Sacramento CA 95814

**Re: SB 813 (McNerney) California Artificial Intelligence Standards and Safety
Commission: artificial intelligence safety standards. – OPPOSED**

Dear Senator McNerney:

The Business Software Alliance appreciates the opportunity to share insights from the enterprise software sector on SB 813. BSA is the leading advocate for the global software industry.¹ BSA members are at the forefront of developing cutting edge services, and their products are used by businesses of all sizes across every sector of the economy.

AI is changing the way we live and work, and it has real-world benefits. Realizing the potential of AI requires trusting that the technology is developed and deployed responsibly. Crafting AI legislation that promotes responsible uses of AI and protects against misuse is one of the most important technology issues today. As policymakers consider how to regulate AI, it is important that new requirements are risk-based, workable in practice, and interoperable with national and international approaches.

BSA supports strong, risk-based AI governance that protects consumers and gives companies clear, workable obligations. However, we continue to oppose SB 813 because:

- Creating a state-specific independent verification organization (IVO) framework remains premature given the evolving AI assurance ecosystem;
- The bill does not establish adequate safeguards to ensure the competence and credibility of state-designated IVOs;
- California should build on international and national standards and accreditation processes rather than establish a separate, state-specific regime;
- The bill gives undefined “identified standards” significance in civil litigation, creating uncertainty and potentially making voluntary audits a de facto expectation; and

¹ BSA's members include: Adobe, Alteryx, Amadeus, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., TrendAI, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

- Long-used accountability tools, like impact assessments and risk management programs, can help ensure companies develop and deploy AI responsibly, without creating the concerns caused by third-party audits.

We welcome the significant amendments to SB 813 made on August 24. In particular, the amendments appropriately remove the proposed California Artificial Intelligence Standards and Safety Commission and provisions directing the state to develop minimum compliance and advanced safety standards. The amendments also make clear that a developer or deployer is not required to engage an independent verification organization (IVO) or undergo a covered AI audit as a condition of developing, deploying, or operating an AI system in California. The bill, however, continues to raise significant concerns, which we explain in more detail below.

I. Creating A State-Specific Framework for IVOs Remains Premature

SB 813 directs the Government Operations Agency (GovOps) to develop requirements for IVOs, determine which entities qualify for registration, and establish procedures for suspending or terminating an IVO's registration. Such an approach is premature. California has not established a general requirement for private-sector AI audits, nor has the Legislature determined which AI uses warrant independent third-party verification or what an audit should evaluate in those circumstances. Yet SB 813 directs the state to begin establishing a new category of government-designated AI assurance providers now.

AI auditing and assurance remain developing fields. Methodologies differ based on the type of AI system, the risks being evaluated, the context in which the system is deployed, and the purpose of the assessment. Creating a state designation regime before these practices have sufficiently matured risks prematurely privileging particular methodologies, benchmarks, or approaches. It also risks creating expectations that a state-designated IVO is necessary even in contexts where other accountability mechanisms are more appropriate.

BSA supports meaningful accountability for AI, particularly for high-risk uses that can significantly affect consumers. But accountability requirements should respond to identified risks. Policymakers should first determine whether and where independent verification is necessary before creating a regulatory infrastructure to govern the organizations that might perform it.

II. Ensuring the Competence and Credibility of Auditors Is Critical

The credibility of any independent verification regime ultimately depends on the quality of the organizations performing the assessments. However, SB 813 provides few objective minimum qualifications for an entity seeking designation as an IVO.

The bill directs GovOps to develop criteria and to consider whether an applicant is capable of assessing AI risks, employs personnel with sufficient technical expertise, and can identify and manage conflicts of interest. Those are important considerations, but they leave substantial questions unanswered. The bill does not require an applicant to demonstrate a minimum level of experience conducting AI assessments, establish a record of successfully performing comparable engagements, obtain accreditation under a recognized conformity-assessment framework, or demonstrate that its methodologies have been independently validated.

Additionally, the bill does not establish meaningful statutory criteria for evaluating whether an applicant's proposed benchmarks, metrics, and methodologies are technically sound. Instead, applicants submit information about the methodologies they propose to use, and GovOps is left to develop the requirements by which those applicants will be evaluated.

The bill therefore risks conferring a government designation to organizations whose expertise, methodologies, and track records vary substantially. A state designation can itself convey credibility to customers, courts, and the public. California therefore should not establish an IVO designation unless it can ensure that the designation reflects rigorous, objective, and consistently applied qualifications.

This concern further demonstrates why California should build on established national and international accreditation and conformity-assessment processes rather than create a new state-specific designation.

III. Governments Should Support International Standards, Rather Than Diverge from Them

SB 813 risks causing California to diverge from consensus-based, international AI standards. AI is developed and deployed across state and national borders. As a result, standards governing AI assurance and independent verification should be interoperable with internationally recognized approaches, to create clarity for businesses and consumers.

We appreciate that SB 813 directs GovOps to identify and consider standards, frameworks, guidelines, criteria, and best practices developed by national and international auditing and assurance organizations. The bill also directs GovOps, "to the extent practicable," to align the procedures and criteria it develops with existing professional and regulatory audit and assurance standards and frameworks.

While the reference to other standards and frameworks is important, the bill does not adequately ensure alignment. SB 813 ultimately leaves GovOps responsible for developing

the criteria that determine whether an AI auditor qualifies as a registered IVO, and the bill does not require those criteria to conform to internationally recognized standards or provide a clear basis for determining when California-specific requirements are necessary. As a result, the IVO framework established by the bill could evolve in ways that depart from internationally developed standards and accepted assurance practices.

That outcome would risk making California an outlier at a time when greater consistency is needed. International standards development processes are designed to bring together technical expertise and stakeholder perspectives across jurisdictions and to promote consistency, comparability, and reliability. Across every industry sector, international standards organizations like the International Organization for Standardization (ISO) and Institute of Electrical and Electronics Engineers (IEEE) create new standards as needs arise. Before a new standard is proposed, there is often significant foundational work by a range of experts, including technical research, to explore the activities that ought to be standardized.

AI standards should be created through the same international standards development process used across industries and technologies. Several international AI standards development activities are already underway. For example, the ISO/IEC JTC1/SC 42 is tasked with developing technical standards and guidelines for AI and has already published more than 20 AI-related standards. Governments should support these standards development processes rather than creating frameworks that could diverge from them.

IV. Clarifying the Legal Significance of AI Audits Is Paramount to the Bill's Express Intent of Ensuring AI Audits Are Voluntary

SB 813 directs GovOps to convene working groups to solicit stakeholder input in the “identification of standards.” The bill also provides that, in an action alleging that the development, modification, or use of an AI system caused harm, the fact that an audit was performed in accordance with a standard identified under the chapter is relevant to the action.

The bill does not, however, establish a clear process for determining which standards are “identified” for this purpose. It does not specify who formally identifies a standard, what criteria govern that determination, whether identification occurs through a formal administrative process, or how a court should determine whether a particular standard applies to the AI system and alleged harm at issue.

Those ambiguities are especially concerning because the bill gives these standards potential significance in litigation. Consensus-based, international standards can provide valuable tools for organizations seeking to manage risk, but California should not give an undefined category of technical standards legal significance without clear rules governing their identification and application.

The provision may also undermine the bill's express statement that audits are voluntary. Although SB 813 provides that a company is not required to engage an IVO or undergo a covered AI audit, expressly directing courts to consider the existence of an audit may create substantial practical pressure for companies to obtain audits defensively.

If the Legislature intends SB 813's framework to remain voluntary, the bill should at minimum make clear that the absence of an audit, the decision not to engage an IVO, or the failure to follow a standard identified under the chapter may not independently be used to establish negligence, fault, or liability.

V. Long-Used Accountability Tools Can Help Ensure Companies Develop and Deploy AI Responsibly

SB 813 bypasses proven accountability tools, such as impact assessments, in favor of establishing a framework for third-party AI audits, before the Legislature has even established which uses of AI warrant external verification. We agree that accountability in AI is important, particularly for high-risk uses of AI that have the most significant impacts on consumers' daily lives, and encourages the Legislature to focus on long-used accountability tools that do not create the same concerns caused by third-party audits.

For high-risk scenarios, new safeguards are important—and legislation can leverage tools that already exist to help companies identify and mitigate potential risks. BSA supports requiring companies that develop or deploy AI for high-risk uses to: (1) adopt risk management programs; and (2) conduct impact assessments. These measures can help companies identify and mitigate risks when AI makes important decisions about consumers—and increase trust that AI is developed and used responsibly. In particular:

- Risk management programs establish repeatable processes for companies to identify and mitigate potential risks that can arise throughout the lifecycle of an AI system. Risk management is particularly important in contexts like AI, privacy, and cybersecurity, where the combination of quickly evolving technologies and highly dynamic threat landscapes can render traditional approaches to compliance ineffective. One way for companies to establish risk management programs is by using the AI Risk Management Framework (AI RMF), developed by the National Institute of Standards and Technology (NIST). The AI RMF builds on NIST's work creating frameworks for managing cybersecurity and privacy risks. Ultimately, effective AI risk management programs should support cross-company coordination to promote the identification and mitigation of risks across the lifecycle of an AI system.

- Impact assessments are a key part of a meaningful risk management program. Both developers and deployers should use impact assessments as a tool for the responsible development and use of high-risk AI systems—and each type of company should conduct an impact assessment that reflects their role in developing or deploying the AI system. Impact assessments are already widely used in a range of other fields, including privacy, as an accountability mechanism that demonstrates a product or system has been designed in a manner that accounts for the potential risks it may pose to the public. Because impact assessments already exist today in other fields, they can be readily adapted to help companies identify and mitigate AI-related risks.²

For these reasons, BSA is opposed to SB 813.

* * *

Thank you for allowing us to provide the enterprise software sector's perspective on SB 813. We welcome the opportunity to further engage with you or a member of your staff on these important issues.

Sincerely,

Meghan Pensyl
Director, Policy

² See BSA, Impact Assessments: A Key Part of AI Accountability, *available at* <https://www.bsa.org/policy-filings/impact-assessments-a-key-part-of-ai-accountability>.