SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2025-2026 Regular Session

AB 1405 (Bauer-Kahan)
Version: April 3, 2025
Hearing Date: July 1, 2025
Fiscal: Yes
Urgency: No
CK

SUBJECT

Artificial intelligence: auditors: enrollment

DIGEST

This bill establishes an enrollment process for auditors of AI systems or models through the Government Operations Agency (GovOps) and sets certain minimum standards for AI auditing pursuant to any state statutes.

EXECUTIVE SUMMARY

AI models and systems have opened beneficial possibilities and breakthroughs in a variety of sectors, including healthcare, creative industries, education, business operations, and customer service. However, these models also pose significant risks to society with their capabilities, whether it is through the creation of chemical, biological, radiological, or nuclear (CBRN) weapons, utilization to carry out cyberattacks at scale, algorithmic discrimination, or evasion of the oversight and control of their developers or deployers. Given how complex and opaque these models can be and the lack of comprehensive regulatory oversight of their development, one tool that has increasingly been advocated for as a foundational element of any such framework is the use of independent auditing.

In order to ensure the proper oversight and identification of sophisticated and reliable AI auditors should such auditing be required by law in the future, this bill establishes a process for GovOps to enroll AI auditors and create a publicly accessible listing of relevant information about these auditors. The bill provides clear guidelines for "covered audits" and a number of requirements to ensure no conflict of interests or misconduct on the part of enrolled AI auditors. This bill is author-sponsored and supported by Oakland Privacy and Transparency Coalition.ai. It is opposed by industry associations, including TechCA. Should the bill pass this Committee it will then be referred to the Senate Governmental Organization Committee.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Establishes the Government Operations Agency (GovOps) within the state government. (Gov. Code § 12800.)

2) Establishes the Department of Technology within GovOps, and charges it with the approval and oversight of information technology projects. (Gov. Code §§ 11545, 11546.)

3) Defines "artificial intelligence" as an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments. (Gov. Code § 11546.45.5(a)(1).)

This bill:

1) Requires GovOps, by January 1, 2027, to do all of the following:
   a) Establish mechanisms on their website allowing AI auditors to enroll and natural persons to report misconduct by an enrolled AI auditor.
   b) Fix enrollment fees at an amount not exceeding the reasonable costs of administering these provisions.

2) Requires GovOps, starting January 1, 2027, to do all of the following:
   a) Publish any information provided by an enrolled AI auditor in a publicly accessible format on the agency's website.
   b) Retain any report submitted using the relevant mechanism for as long as the enrolled AI auditor remains enrolled, plus 10 years.
   c) Share reports submitted using the relevant mechanism with other state agencies as necessary for enforcement purposes.

3) Requires an AI auditor, beginning January 1, 2027, prior to conducting any covered audits, to do all of the following:
   a) Enroll with GovOps and pay the relevant enrollment fee.
   b) Provide GovOps with specified information, including details about the AI auditor and their protocols.

4) Defines "covered audit" as an audit conducted pursuant to any state statute that requires an audit of an AI system or model by an independent third party auditor.

5) Requires an AI auditor, in conducting a covered audit, to abide by generally accepted industry best practices appropriate to the system or model being audited.

6) Requires an AI auditor, after conducting a covered audit, to provide the auditee with an audit report that contains, but is not limited to, all of the following:
   a) The scope and objectives of the audit.
   b) The results of the audit and any documentation necessary to demonstrate the basis of those results.
   c) An explanation of any steps the auditee can take to meet generally accepted industry standards appropriate to the system or model being audited.
   d) An explanation of any steps the auditee can take to become compliant with state law.
   e) A statement that is signed and dated by each auditor that certifies that the covered audit was completed.

7) Prohibits an AI auditor from knowingly making a material misrepresentation in an audit report prepared pursuant hereto. An enrolled AI auditor shall not conduct a covered audit if it has a financial interest in the auditee other than financial compensation for performing an audit.

8) Requires an enrolled AI auditor to retain any documentation that is provided to an auditee pursuant to this chapter, or that is necessary to demonstrate the basis of the result of a covered audit, for at least 10 years.

9) Provides that an enrolled AI auditor shall not accept employment with an auditee within 12 months of completing a covered audit of the auditee. An enrolled AI auditor shall not conduct a covered audit if the auditee had employed the auditor during the 12-month period preceding the audit.

10) Authorizes an enrolled AI auditor to disclose confidential information concerning an auditee only if the auditee provides written authorization or if the disclosure is any of the following:
    a) Made in compliance with a subpoena or a summons enforceable by order of a court.
    b) Reasonably necessary to maintain or defend the auditor in a legal proceeding initiated by the auditee.
    c) Made in response to an official inquiry from a federal or state government regulatory agency.
    d) Made to another enrolled AI auditor or person in connection with a proposed sale or merger of the auditor's professional practice, provided the parties enter into a written nondisclosure agreement with regard to all auditee information shared between the parties.

e) Made to another enrolled AI auditor to the extent necessary for purposes of professional consultation.
f) Made to organizations that provide professional standards review and ethics or quality control peer review.
g) Specifically permitted by state or federal law.

11) Provides that an enrolled AI auditor shall not do either of the following:
a) Prevent an employee from disclosing information to the Attorney General or the Labor Commissioner, or using the misconduct-reporting mechanism, including through terms and conditions of employment or seeking to enforce terms and conditions of employment, if the employee has reasonable cause to believe the information indicates that the auditor is out of compliance with the requirements of this chapter.
b) Retaliate against an employee for so disclosing information.

12) Establishes the AI Auditors' Enrollment Fund within the State Treasury. The fund shall be administered by GovOps and all moneys collected or received by the agency hereunder shall be deposited into this fund to be available for expenditure by GovOps, upon appropriation by the Legislature, to administer this program.

COMMENTS

1. The use of independent audits for proper AI oversight

The use of AI auditing can be a key tool in effectively assessing how AI systems and models are working and what their impacts are. Audits can ensure legal compliance and, when shared publicly, afford a measure of transparency. Mandatory audits create baseline standards across the industry, making it easier to compare different AI systems and ensuring minimum safety thresholds. This levels the playing field and prevents a "race to the bottom" where competitive pressures lead companies to skimp on safety measures. Audit requirements create transparency that builds public confidence in AI systems, especially those used in critical domains like healthcare, criminal justice, or financial services. When people know systems have been independently verified, they are more likely to accept and appropriately use AI tools. This accountability also provides recourse when things go wrong, as qualified auditors can provide concrete evidence for regulatory decisions and legal proceedings. They create a paper trail showing whether companies exercised reasonable care, which is crucial for determining liability when AI systems cause harm. Especially given the limited resources and expertise of state government in carrying out such audits, ensuring the availability of qualified independent auditors is crucial to the effectiveness of any auditing regime.

Last year, the National Telecommunications and Information Administration (NTIA) published an "Artificial Intelligence Accountability Policy Report." One of its main recommendations focused on the utility of such independent auditing:

> Independent AI audits and evaluations are central to any accountability structure. To help create clarity and utility around independent audits, we recommend that the government work with stakeholders to create basic guidelines for what an audit covers and how it is conducted – guidance that will undoubtedly have some general components and some domain-specific ones. This work would likely include the creation of auditor certifications and audit methodologies, as well as mechanisms for regulatory recognition of appropriate certifications and methodologies.
>
> Auditors should adhere to consensus standards and audit criteria where possible, recognizing that some will be specific to particular risks (e.g., dangerous capabilities in a foundation model) and/or particular deployment contexts (e.g., discriminatory impact in hiring). Much work is required to create those standards – which NIST and others are undertaking. Audits and other evaluations are being rolled out now concurrently with the development of technical standards. Especially where evaluators are not yet relying on consensus standards, it is important that they show their work so that they too are subject to evaluation. Auditors should disclose methodological choices and auditor independence criteria, with the goal of standardizing such methods and criteria as appropriate. The goals of safeguarding sensitive information and ensuring auditor independence and appropriate expertise may militate towards a certification process for qualified auditors.
>
> AI audits should, at a minimum, be able to evaluate claims made about an AI system's fitness for purpose, performance, processes, and controls.[1]

2. Establishing an enrollment process for AI auditors

This bill establishes the infrastructure for overseeing the auditing of AI systems and models as may be required by California law, implementing a number of elements recommended by the NTIA report.

The bill tasks GovOps with setting up mechanisms for AI auditors to enroll and pay an established fee before conducting "covered audits," defined as audits conducted pursuant to any state statute that requires an audit of an AI system or model by an

[1] *Artificial Intelligence Accountability Policy Report* (March 27, 2024) NTIA, https://www.ntia.gov/sites/default/files/publications/ntia-ai-report-final.pdf [as of June 26, 2025].

independent third party auditor. Currently, no such auditing requirements exist, but they are currently being contemplated in pending legislation.

In order to carry out covered audits, enrolled AI auditors must provide GovOps with specified information about themselves. This includes not only identifying and contact information, but also the types of AI systems or models that the auditor is enrolling to audit and any relevant certifications or accreditations and the identities of the certifying or accrediting entities. They must also provide a written description of the auditor and the services they provide, not to exceed 200 words in length. AI auditors must also include a standard operating procedure (SOP) that describes their procedures in sufficient detail to enable a third party to assess whether audits are conducted according to generally accepted industry best practices. GovOps is required to publish this information and make it publically available.

The bill also prescribes necessary elements of AI audits that must be provided to the auditee, including:

- The scope and objectives of the audit.
- The results of the audit and any documentation necessary to demonstrate the basis of those results.
- An explanation of any steps the auditee can take to meet generally accepted industry standards appropriate to the system or model being audited.
- An explanation of any steps the auditee can take to become compliant with state law.
- A statement that is signed and dated by each auditor that certifies that the covered audit was completed.

The bill includes several provisions working to ensure ethical and accountable auditing. Enrolled AI auditors must abide by generally accepted industry best practices. GovOps is required to establish a mechanism allowing for reports of AI auditor misconduct and to retain those for at least 10 years beyond the time an auditor is enrolled. Any submitted reports must be shared with other state agencies as needed for enforcement purposes. Employees cannot be prevented from, or retaliated against for, disclosing relevant information to the Attorney General or Labor Commissioner, or making reports through the misconduct-reporting mechanism.

Auditors are prohibited from knowingly making material misrepresentations and shall not conduct a covered audit if they have a financial interest in the auditee other than financial compensation for performing an audit. To prevent possible collusion, an enrolled AI auditor shall not accept employment with an auditee within a year of completing a covered audit of the auditee or conduct a covered audit if the auditee had employed the auditor during the 12-month period preceding the audit.

To protect confidential information of the auditee, the bill places strict limits on when an enrolled AI auditor can disclose such information, such as in response to a subpoena or official inquiry of government regulators or with the written authorization of the auditee.

According to the author:

> Over the past decade, artificial intelligence (AI) systems have become increasingly powerful and accessible. Just as financial audits improve transparency and mitigate risks in capital markets, independent third party audits play a critical role in ensuring that AI systems are developed and deployed responsibly. Well-structured audits can help identify risks, verify compliance with ethical and legal standards, and build public trust in AI technologies. AB 1405 establishes an enrollment process for AI auditors and sets minimum transparency, competency, and ethical standards for enrolled auditors.

3. <u>Stakeholder positions</u>

Writing in support, Oakland Privacy asserts:

> Assembly Bill 1405 addresses the large question of how all of the companies that will have to start performing risk assessments under proposed regulations at both the CA Privacy Protection Agency, and on the legislative agenda, will find qualified auditors. While we firmly believe that the creation of new markets causes human beings to pivot to fill the void, it makes perfect sense for the State to help such organic processes along.
>
> AB 1405 proposes a registry that would provide in one place the experiences and qualifications of a number of third party entities who are available to take on this work and allows businesses, especially those who may never have undertaken a risk assessment audit before, to get a handle on how to contract for this service.
>
> We are always glad to see the Legislature making an effort to produce useful compliance resources and we think this makes a great deal of sense. It is always more cost-effective and more helpful to the people of the State to aid regulatory compliance as opposed to penalizing for noncompliance.

The Business Software Alliance writes in opposition:

> [T]he existing AI auditing ecosystem is immature. While existing state law requires audits of certain public-sector high-risk automated decision systems, proposed legislation, namely AB 1018, would require third-party audits of private-sector automated decision systems. We have concerns

> regarding requirements for third-party audits of private-sector AI systems because today's AI auditing ecosystem is nascent and lacks: (1) comprehensive standards for how AI audits should be conducted; (2) a robust framework for governing the professional conduct of AI auditors; and (3) sufficient resources for conducting AI audits. Establishing clear mechanisms for audits of government AI systems that are already required by current law may help ensure those audits are conducted efficiently, however, we are concerned by any legislation that seeks to create auditing regimes for private-sector AI systems and encourage policymakers to consider more widely used and workable accountability tools, like impact assessments.

A coalition of industry groups, including Technet, write in opposition:

> While protecting whistleblowers obviously serves important policy objectives in any number of contexts, these provisions are both unnecessary and potentially counterproductive in this context. Existing frameworks, including the Sarbanes-Oxley Act and California Labor Code Section 1102.5, already provide robust protection for employees who report wrongdoing and there is no reason to believe that these protections are insufficient. There is nothing unique or inherent to the use of AI that justifies creating an overlapping, if not inconsistent schemes for a subset of auditors. To the contrary, imposing duplicative rules risks confusing reporting pathways for workers and creating compliance uncertainty. It may even suggest that existing laws would not apply in the absence of creating new protections such as these.

TechEquity Action writes in support of the bill:

> AI audits can provide crucial independent verification that consequential AI systems function as claimed and mitigate the risk of bias and unintended harms. Without this specialized oversight, we risk allowing potentially harmful systems to impact millions of people with insufficient scrutiny or accountability. A clear example of this need can be seen in healthcare and government where automated systems with error rates of over 90% have impacted access to unemployment benefits and health insurance. Independent AI audits may have caught these errors before they resulted in denied claims, fraud accusations and lawsuits.
>
> AI auditing is a relatively new field that needs structure and standards to grow. AB 1405 provides a needed framework for AI auditing that would:
>
> 1. **Create standardized practices for AI auditing**, establishing a professional ecosystem of qualified, independent auditors and

helping to document and advance industry best practices regarding AI audits.
2. **Decrease litigation risks and costs** for both companies and consumers by identifying and addressing potential issues early, before they lead to harm requiring legal remedies.
3. **Foster greater trust in AI technologies** among consumers and businesses alike, driving responsible innovation and adoption of responsible AI.
4. **Create a new professional sector** of AI auditors to drive accountability, much like financial auditors do, generating high-quality jobs in California and greater trust in these systems.

SUPPORT

Oakland Privacy
TechEquity Action
Transparency Coalition.ai

OPPOSITION

Business Software Alliance
California Chamber of Commerce
Computer and Communications Industry Association
Techca
Technet

RELATED LEGISLATION

Pending Legislation:

SB 420 (Padilla, 2025) regulates the use of "high-risk automated decision systems (ADS)." This includes requirements on developers and deployers to perform impact assessments on their systems. SB 420 establishes the right of individuals to know when an ADS has been used, details about the systems, and an opportunity to appeal ADS decisions, where technically feasible. SB 420 is currently in the Assembly Privacy and Consumer Protection Committee.

SB 468 (Becker, 2025) imposes a duty on a business that deploys a high-risk artificial intelligence system, or high-risk ADS, that processes personal information to protect that information and requires such a deployer to maintain a comprehensive information security program that meets specified requirements. SB 468 is currently in the Senate Appropriations Committee.

SB 813 (McNerney, 2025) provides a rebuttable presumption against liability for harms caused by an AI model or application if it is certified by a private “multistakeholder regulatory organization” that is designated by the Attorney General, as provided. SB 813 is currently in the Senate Appropriations Committee.

AB 1018 (Bauer-Kahan, 2025) regulates the development and deployment of ADS that are used in "consequential decisions" – those that materially impact an individual's rights, opportunities, or access to critical resources or services – in order to mitigate bias and unreliability in these systems. Developers are required to contract with an independent third-party auditor to assess the developer's compliance with requirements for performance evaluations. AB 1018 is currently in this Committee.

Prior Legislation:

SB 1047 (Wiener, 2024) would have, among other things, required developers of powerful AI models and those providing the computing power to train such models to put appropriate safeguards and policies into place to prevent critical harms. It would have established a state entity to oversee the development of these models. SB 1047 was vetoed by Governor Newsom. In his veto message, he stated:

> SB 1047 magnified the conversation about threats that could emerge from the deployment of AI. Key to the debate is whether the threshold for regulation should be based on the cost and number of computations needed to develop an AI model, or whether we should evaluate the system’s actual risks regardless of these factors. This global discussion is occurring as the capabilities of AI continue to scale at an impressive pace. At the same time, the strategies and solutions for addressing the risk of catastrophic harm are rapidly evolving.
>
> By focusing only on the most expensive and large-scale models, SB 1047 establishes a regulatory framework that could give the public a false sense of security about controlling this fast-moving technology. Smaller, specialized models may emerge as equally or even more dangerous than the models targeted by SB 1047 - at the potential expense of curtailing the very innovation that fuels advancement in favor of the public good.

AB 2885 (Bauer-Kahan & Umberg, Ch. 843, Stats. 2024) established a uniform definition for “artificial intelligence” in California’s code, which is used in this bill.

PRIOR VOTES:

Assembly Floor (Ayes 62, Noes 4)
Assembly Appropriations Committee (Ayes 11, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 11, Noes 1)
****