Date of Hearing: April 1, 2025

Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 1405 (Bauer-Kahan) – As Introduced February 21, 2025

PROPOSED AMENDMENTS

SUBJECT: Artificial intelligence: auditors: enrollment

SYNOPSIS

The use of artificial intelligence is becoming commonplace in many industries where it is used to either augment or supplant human decision makers. This technology has the capability to increase efficiency, cut costs, and streamline many processes. These advances have raised questions in both the private and public sector about how the public can be assured that these systems are deployed safely. Third-party audits of AI systems have recently arisen as a way to sow trust into the system and ensure that AI systems comply with state laws and ethical practices.

This author-sponsored bill would establish an enrollment process for AI auditors within the Government Operation Agency. The bill neither mandates audits nor prescribes how audits are to be carried out. Instead, it creates a publicly accessible repository of AI auditors and requires that they adhere to minimum standards of transparency, confidentiality, and ethical conduct. It also provides for whistleblower protections in certain cases. As such, the bill would help promote this burgeoning industry, enable California to be a leader in developing AI auditing best practices, and foster public trust and accountability in the testing and oversight of AI models and systems.

This bill is supported by Oakland Privacy, The California Initiative for Technology & Democracy (CITED), and Transparency Coalition.AI. The bill has no opposition, although Business Software Alliance has submitted a letter of concern noting the industry is still developing and audits are costly.

Committee amendments set forth in Comment #6 enhance whistleblower protections, clarify transparency requirements, and further restrict the revolving door between auditors and auditees.

THIS BILL:

1) Defines the following terms:

   a. “Agency” to mean the Government Operations Agency.

   b. “Artificial intelligence” or “AI” to mean 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.

c. "Artificial intelligence auditor" or "AI auditor" to mean a person, partnership, or corporation that assesses an AI system or model on behalf of a third party.

d. "Covered audit" to mean an audit conducted pursuant to any state statute that requires an audit of an AI system or model by an independent third party auditor.

2) Establishes the AI Auditors' Enrollment Fund is within the State Treasury. The fund will be administered by the Government Operations Agency.

3) Requires that the agency do all of the following by January 1, 2025:

   a. Establish a mechanism on the agency's internet website allowing AI auditors to enroll with the agency.

   b. Fix enrollment fees at an amount not exceeding the reasonable costs of administering the bill.

   c. Establish a mechanism on the agency's internet website allowing natural persons to report misconduct by an enrolled AI auditor.

4) Requires that the agency do both of the following beginning January 1, 2027:

   a. Publish any information provided by an enrolled AI auditor in a publicly accessible format on the agency's internet website.

   b. Retain any report submitted pertaining to an enrolled AI auditor for as long as the auditor remains enrolled, plus 10 years.

5) Requires that prior to initially conducting a covered audit, an AI auditor must do all of the following beginning January 1, 2027:

   a. Enroll with the agency.

   b. Pay the agency the enrollment fee.

   c. Provide to the agency all of the following information:

      i. The name of the auditor.

      ii. All of the following contact information:

         1. The primary physical address of the auditor, if the auditor has a physical address.

         2. The primary internet website of the auditor, if the auditor has an internet website.

         3. A telephone number enabling a natural person to communicate with the auditor.

4. An email address enabling a natural person to communicate with the auditor.

iii. The types of AI systems or models that the auditor is qualified to audit.

iv. Any relevant qualifications, certifications, or accreditations the auditor wishes to provide.

v. A written description of the auditor and the services they provide, not to exceed 200 words in length.

vi. A standard operating procedure (SOP) that describes the auditor's procedures in sufficient detail to enable a third party to assess whether audits are conducted according to generally accepted industry best practices.

6) Requires that an enrolled AI auditor abide by generally accepted industry best practices appropriate to the system or model being audited when conducting a covered audit.

7) Requires that after conducting a covered audit, an enrolled AI auditor provide the auditee with an audit report that contains, but is not limited to, all of the following:

   a. The results of the audit.

   b. An explanation of any steps the auditee can take to meet generally accepted industry standards appropriate to the system or model being audited.

   c. An explanation of any steps the auditee can take to become compliant with state law.

8) Prohibits an AI auditor from knowingly making a material misrepresentation in an audit reportn.

9) Requires an enrolled AI auditor to retain any documentation provided to an auditee pursuant to the bill for at least 10 years.

10) Prohibits an enrolled AI auditor from conducting a covered audit if it has a financial interest in the auditee other than a financial interest that is necessary for the performance of the audit.

11) Prohibits an enrolled AI auditor from accepting employment with an auditee within 12 months of completing a covered audit of the auditee.

12) Provides that an enrolled AI auditor may 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 either of the following:

i. Another enrolled AI auditor to the extent necessary for purposes of professional consultation.

ii. Organizations that provide professional standards review and ethics or quality control peer review.

f. Specifically permitted by state or federal law.

13) Prohibits an enrolled AI auditor from doing either of the following:

a. Prevent an employee from disclosing information to the Attorney General or the Labor Commissioner, or using the mechanism established in this bill, 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 disclosing information.

EXISTING LAW:

1) Establishes the Government Operations Agency. (Gov. Code § 12800.)

2) Establishes the Department of Technology within the Government Operations Agency. (Gov. Code § 12803.2.)

3) Charges the Department of Technology with approving and overseeing information technology projects in the state. (Gov. Code § 11546.)

COMMENTS:

1) **Author's statement**. 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.

2) **AI and GenAI.** The development of GenAI is creating exciting opportunities to grow California's economy and improve the lives of its residents. GenAI can generate compelling text, images and audio in an instant – but with novel technologies come novel safety concerns.

In brief, AI is the mimicking of human intelligence by artificial systems such as computers. AI uses algorithms – sets of rules – to transform inputs into outputs. Inputs and outputs can be anything a computer can process: numbers, text, audio, video, or movement. AI is not fundamentally different from other computer functions; its novelty lies in its application. Unlike normal computer functions, AI is able to accomplish tasks that are normally performed by humans.

AI that are trained on small, specific datasets in order to make recommendations and predictions are sometimes referred to as "predictive AI." This differentiates them from GenAI, which are trained on massive datasets in order to produce detailed text and images. When Netflix suggests a TV show to a viewer, the recommendation is produced by predictive AI that has been trained on the viewing habits of Netflix users. When ChatGPT generates text in clear, concise paragraphs, it uses GenAI that has been trained on the written contents of the internet.

GenAI tools can be released in open-source or closed-source formats by their creators. Open-source tools are publically available; researchers and developers can access their code and parameters. This accessibility increases transparency, but it has downsides: when a tool's code and parameters can be easily accessed, they can be easily altered, and open-source tools have the potential to be used for nefarious purposes such as generating deepfake pornography and targeted propaganda. By comparison, closed-source tools are opaque with respect to their security features. It is harder for bad actors to generate illicit materials using these tools. But unlike open-source tools, closed-source tools are not subject to collective oversight because their inner workings cannot be examined by independent experts.

3) **The Case for Auditing**. Auditing may evoke visions of the IRS pursuing individuals or corporations for fraudulent tax practices, but audits are commonplace in numerous fields. Even the idea of auditing an algorithm itself is not new. In the 1960s, American Airlines began using a rudimentary computer program to aid in the booking of flights, which streamlined the process for travel agents and prevented double bookings. American Airlines extended this program to other airlines in the 1980s; however, an audit of this program discovered that the algorithm ensured that American Airlines flights would show up as the top result in any search, regardless of whether they were longer or more expensive. During a US Congressional investigation into this business practice, the President of American Airlines did not deny that the algorithm prioritized their flights. Instead, he doubled down, stating that "the preferential display of our flights, and the corresponding increase in our market share, is the competitive raison d'etre for having created the system in the first place".[1] Although regulations were ultimately put in place to address this algorithmic bias in flight offerings, there remains little to no legislative oversight for algorithms deployed in other sectors.

Algorithms and AI systems are usually evaluated for their outputs, meaning most testing focuses on whether the output matches with the desired outcome of the deployer. However, this approach results in a simplistic binary pass/fail assessment rather than a systematic analysis aimed at understanding the underlying issues with the algorithm. Audits of AI systems have often been in response to investigative journalism or public outcry.

[1] Christian Sandvig et al, "Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms," *Data and Discrimination: Converting Critical Concerns into Productive Inquiry* (May 22, 2014), accessed at https://kevinhamilton.org/.

For instance, ProPublica reported in 2016 that a commercially available algorithm used to assess the likelihood of recidivism among criminals predicted that Black individuals had a 77% higher likelihood of recidivism than white individuals, even when controlling for prior crimes, age, gender and actual recidivism. This finding suggested that race alone significantly influenced the algorithm's output, and led to a reevaluation of the use of this algorithm.[2] Similarly, in 2020, Twitter introduced an AI-powered image cropping tool designed to center photos to try to highlight faces or other interesting elements. However, users quickly observed that the tool disproportionately favored white faces over Black faces and women over men. Twitter quickly launched their own study and found that this bias was indeed present.[3]

These two cases were among the most widely publicized examples of algorithmic bias. However, most AI systems are "black boxes," concealed by company trade secrets, making it difficult for the public to evaluate whether these systems are being used legally and ethically. Testing these systems becomes challenging when only the output is accessible, especially as the number of variables involved increases. For example, it is easy to verify if a calculator is adding two numbers correctly, but when an algorithm is used to assess college admissions, considering factors such as essays, grades, extracurricular activities, and other criteria, it becomes nearly impossible to understand why a certain outcome occurred. Determining whether bias influenced the outcome is even more difficult without access to extensive data. This makes it practically impossible for anyone to hold these systems accountable from the outside.

This is especially crucial as AI systems proliferate and expand into more industries, where misuse could have even graver consequences. The major risks associated with AI deployment have been summarized in the National Institute of Standards and Technology's "Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile" as follows:

> 1. CBRN Information or Capabilities: Eased access to or synthesis of materially nefarious information or design capabilities related to chemical, biological, radiological, or nuclear (CBRN) weapons or other dangerous materials or agents.
>
> 2. Confabulation: The production of confidently stated but erroneous or false content (known colloquially as "hallucinations" or "fabrications") by which users may be misled or deceived.
>
> 3. Dangerous, Violent, or Hateful Content: Eased production of and access to violent, inciting, radicalizing, or threatening content as well as recommendations to carry out self-harm or conduct illegal activities. Includes difficulty controlling public exposure to hateful and disparaging or stereotyping content.
>
> 4. Data Privacy: Impacts due to leakage and unauthorized use, disclosure, or de-anonymization of biometric, health, location, or other personally identifiable information or sensitive data.
>
> 5. Environmental Impacts: Impacts due to high compute resource utilization in training or operating GAI models, and related outcomes that may adversely impact ecosystems.

[2] Jeff Larson et al., "How We Analyzed the COMPAS Recidivism Algorithm," *ProPublica* (May 23, 2016), access at https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm.

[3] Rumman Chowdhury, "Sharing learnings about our image cropping algorithm", *X Engineering* (May 19, 2021), accessed at https://blog.x.com/engineering/en_us/topics/insights/2021/sharing-learnings-about-our-image-cropping-algorithm.

6. Harmful Bias or Homogenization: Amplification and exacerbation of historical, societal, and systemic biases; performance disparities between sub-groups or languages, possibly due to non-representative training data, that result in discrimination, amplification of biases, or incorrect presumptions about performance; undesired homogeneity that skews system or model outputs, which may be erroneous, lead to ill-founded decision-making, or amplify harmful biases.

7. Human-AI Configuration: Arrangements of or interactions between a human and an AI system which can result in the human inappropriately anthropomorphizing GAI systems or experiencing algorithmic aversion, automation bias, over-reliance, or emotional entanglement with GAI systems.

8. Information Integrity: Lowered barrier to entry to generate and support the exchange and consumption of content which may not distinguish fact from opinion or fiction or acknowledge uncertainties, or could be leveraged for large-scale dis- and mis-information campaigns.

9. Information Security: Lowered barriers for offensive cyber capabilities, including via automated discovery and exploitation of vulnerabilities to ease hacking, malware, phishing, offensive cyber operations, or other cyberattacks; increased attack surface for targeted cyberattacks, which may compromise a system's availability or the confidentiality or integrity of training data, code, or model weights.

10. Intellectual Property: Eased production or replication of alleged copyrighted, trademarked, or licensed content without authorization (possibly in situations which do not fall under fair use); eased exposure of trade secrets; or plagiarism or illegal replication.

11. Obscene, Degrading, and/or Abusive Content: Eased production of and access to obscene, degrading, and/or abusive imagery which can cause harm, including synthetic child sexual abuse material (CSAM), and nonconsensual intimate images (NCII) of adults.

12. Value Chain and Component Integration: Non-transparent or untraceable integration of upstream third-party components, including data that has been improperly obtained or not processed and cleaned due to increased automation from GAI; improper supplier vetting across the AI lifecycle; or other issues that diminish transparency or accountability for downstream users. [4]

Many of these harms of AI are currently being considered by the legislature including obscene and abusive content (AB 671, Bauer-Kahan), Intellectual Property (AB 412, Bauer-Kahan), Data Privacy (SB 468, Becker), environmental impacts (AB 222, Bauer-Kahan and AB 93, Papan), human-AI configurations (AB 1064, Bauer-Kahan, AB 410, Wilson, AB 489, Bonta, and SB 243, Padilla) among a myriad of other AI focused legislation. Notably, three bills would require audits, AB 1018 (Bauer-Kahan) addressing algorithmic discrimination and AB 1064 (Bauer-Kahan) and SB 243 (Padilla) addressing human-AI Configurations. As AI continues to develop,

[4] National Institute of Standard and Technology, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," accessed at https://www.nist.gov/news-events/news/2023/01/nist-risk-management-framework-aims-improve-trustworthiness-artificial.

more legislation is likely to arise that addresses AI harms and would require auditing to ensure compliance.

4) **What this bill would do.** This bill would establish an enrollment process within the Government Operations Agency (GovOps) for AI auditors. Enrolled auditors could then perform "covered audits," which are audits mandated by the legislature or regulations. This bill would establish a central repository within GovOps through which one could find an auditor. This bill stipulates that GovOps will establish a publicly accessible format for accessing this repository, as well as a mechanism for reporting auditor wrongdoing. It requires enrolling auditors to disclose information regarding their practice, including contact information, the AI systems and models they are enrolling to audit, any accreditations they may have, and their standard operating procedures. Moreover, this bill mandates that auditors disclose to the auditee the results of audits, the steps auditees can take to bring audited systems into compliance with industry standards and state law, and any necessary corrective actions. The bill also prohibits auditors from knowingly misrepresenting audits and imposes limits on their financial interests and employment with auditees. Lastly, it specifies the circumstances under which auditors may disclose confidential information about an auditee, including compliance with subpoenas and responses to federal or state regulators.

5) **If you build it, will they come?** In a letter of concern from the Business Software Alliance states:

> 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.

While this field is nascent, there already exist many AI auditing firms. This is largely a result of the passage of New York City's "Automated Employment Decision Tools" local law in 2021 that requires audits of tools used in the hiring process for any job in New York City.[5] These AI auditors include Holistic AI, Rocket-Hire, and Babl.[6] The number of auditing entities is likely to increase as AI audits become more common. Individuals can also become certified by the Institute of Internal Auditors, the Information Systems Audit and Control Association, and the International Federation of Global & Green Information & Communication Technology, among a growing number of programs in the auditing and cybersecurity industries.[7]

Moreover, there is a growing desire for third-party oversight from both the public and industry itself. In 2024, a KPMG survey of over 1,800 companies across ten major markets found that 91% of business leaders believe that regular audits are the most effective practice in ensuring ethical AI use. Similarly, 80% of business leaders believe that third-party review will be an integral part of that practice.[8] In fact, many AI companies openly flaunt their use of independent

[5] New York City Law Int 1894-2020, can be read at https://legistar.council.nyc.gov/LegislationDetail.aspx?GUID=B051915D-A9AC-451E-81F8-6596032FA3F9&ID=4344524&Options=&Search=.

[6] Auditors and their websites: Holistic AI (https://www.holisticai.com/), Rocket-Hire (https://rocket-hire.com/ai-bias-audits/), Babl (https://babl.ai/ai-audits/).

[7] These courses are marketed and run by each organization on their respective online webpages.

[8] KPMG, "Navigating The AI Era In Financial Reporting," (May 8, 2024), accessed at https://kpmg.com/us/en/media/news/ai-in-financial-reporting-kpmg-2024.html.

evaluation, such as adversarial testing for harm via red-teaming.[9] This bill would establish a centralized resource that anyone can access and streamline the process for industry to find an auditor. Moreover, this bill legitimizes the growing market of AI auditors that businesses and regulators alike see as a mechanism to ensure safety.

Though the field itself lacks a comprehensive standard, the current practice of developers testing their own AI systems is equally unregulated. These practices are not only opaque, but also depend on first parties acting altruistically rather than, as American Airlines had, in their self-interest. Furthermore, as stated above, industry is likely to encourage third party audits. Overall, there is an understanding that relying solely on internal audits is unlikely to be adequate to ensure that AI systems do not cause harm. The Institute of Internal Auditors in their "Framework for AI Audits" states:

> Internal auditors are not expected to be experts on every audit topic; rather, having a disciplined, methodical approach with a focus on critical thinking and identifying risk should be the objective for all audits, not just AI. Familiarity and a working knowledge of AI is vital; however, knowing all technical aspects of AI is not likely. It may be necessary to engage outside technical resources to assist with more technical aspects such as deciphering algorithms.[10]

As well as bringing in outside expertise, third-party audits are conducted independently, addressing concerns about accuracy in self-reporting. Though, for reports to be accurate, information has to be accessible to the auditor to ensure a comprehensive investigation and report. The Biden Administration's Blueprint for an AI Bill of Rights outlines how these evaluations could be done in regard to automated systems:

> Automated systems should be designed to allow for independent evaluation (e.g., via application programming interfaces). Independent evaluators, such as researchers, journalists, ethics review boards, inspectors general, and third-party auditors, should be given access to the system and samples of associated data, in a manner consistent with privacy, security, law, or regulation (including, e.g., intellectual property law), in order to perform such evaluations. Mechanisms should be included to ensure that system access for evaluation is: provided in a timely manner to the deployment-ready version of the system; trusted to provide genuine, unfiltered access to the full system; and truly independent such that evaluator access cannot be revoked without reasonable and verified justification.[11]

Although no consensus framework exists in the AI auditing space for how such an audit should occur, auditing is not a new field, and auditors could refer to various frameworks already employed by auditors such as the Claims-Arguments-Evidence framework (CAE), which is widely used in safety-critical contexts.[12] These guidelines are relatively flexible and rely on verifiable information for testing. This aligns with the approaches taken by the O'Neil Risk

[9] OpenAI, "OpenAI Red Teaming Network," (Sept. 23, 2023), accessed at https://openai.com/index/red-teaming-network/.
[10] The Institute of Internal Auditors, "Artificial Intelligence Auditing Framework," (Dec. 18, 2023), accessed at https://www.theiia.org/en/content/tools/professional/2023/the-iias-updated-ai-auditing-framework/.
[11] The Biden White House, "Blueprint for an AI Bill of Rights," Oct. 2022, https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/
[12] Miles Brundage et al. "Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims", *arXiv* (Apr. 20, 2020), accessed at https://doi.org/10.48550/arXiv.2004.07213.

Consulting and Algorithmic Auditing firm, which uses adaptive strategies to address the audit at hand.[13] Thus, the bill gives space for auditors and industry to establish "industry best practices" that ensure safety and build trust with the public. Auditing practices are likely to be further developed over the next few years, as audits become more commonplace as other jurisdictions enact similar auditing requirements such as those in the EU AI Act.[14] This enrollment process would ensure that California would be a leader in the development of these best practices.

The recently released draft of the Joint California Policy Working Group on AI Frontier Models, convened by Governor Newsom, highlights the importance of third-party auditing, stating:

> Significant historical experiences with science and technology—inspired by case comparisons to internet policy, consumer products, and energy—highlight the reality that policymaking must often occur under uncertainty. If crafted properly, policymaking under such conditions encourages innovation, pays attention to evidence of both present and emerging risks, and leverages multidisciplinary and thorough assessment of the state of the evidence. Among other implications, the case comparisons underscore the importance of transparency, third-party auditing, and acting on policy windows with mechanisms that surface and enable knowledge and analysis. These insights also highlight the value of augmenting real-world observation with a range of methods to consistently address uncertainty, navigate practical realities, and incorporate critical context from a breadth of perspectives.
>
> […]
>
> Agreement on which risks should be tracked and how they can be measured through evaluations, ideally harmonized to level the playing field through third-party auditing, offers an industry-inspired pathway that can inform governance.[15]

The draft findings of this working group align with the goal of this bill, emphasizing the importance and legitimization of third-party oversight while also empowering the Legislature to work with industry to determine which risks posed by AI can be addressed through audits.

6) **Amendments.** The ultimate goal of this bill is to establish a system that increases transparency and enables accountability in audits. To that end, the author has agreed to various amendments that will clarify or increase transparency and accountability.

The bill acknowledges that auditees have whistleblower rights to ensure that covered audits are performed correctly and therefore provides a mechanism for audited entities to file whistleblower reports against enrolled auditors. However, the bill does not clarify how those reports will be handled. Amendments detailing how these complaints would be handled are as follows:

> (b) Beginning January 1, 2027, the agency shall do **~~both~~*all*** of the following:

[13] Information regarding O'Neil Risk Consulting & Algorithmic Auditing can be found at https://orcaarisk.com/.

[14] Jim Pelletier, "Internal audit's role in the new European Union's Artificial Intelligence Act", *Wolters Kluwer* (June 26, 2024), accessed at https://www.wolterskluwer.com/en/expert-insights/internal-audits-role-new-european-union-ai-act.

[15] Jennifer Tour Chayes, Mariano-Florentino Cuéllar, Li Fei-Fei, "DRAFT REPORT of the Joint California Policy Working Group on AI Frontier Models" (Mar. 18, 2025), accessed at https://www.cafrontieraigov.org/.

(1) Publish any information provided by an enrolled AI auditor pursuant to subdivision (a) of Section 11549.83 in a publicly accessible format on the agency's internet website.

(2) Retain any report submitted using the mechanism established pursuant to paragraph (3) of subdivision (a) ~~pertaining to an enrolled AI auditor~~ for as long as the ***enrolled AI*** auditor remains enrolled, plus 10 years.

(4) Share reports submitted using the mechanism established pursuant to paragraph (3) of subdivision (a) with other state government agencies as necessary for enforcement purposes.

The bill also requires that enrolled auditors provide certain contact information and information regarding credentials. The author has agreed to amendments that would clarify which information is required, such as the auditor's website. Importantly, these amendments will ensure that auditors that have credentials and certifications disclose the source of these qualifications to ensure that they are legitimate:

11549.83. (a) Beginning January 1, 2027, prior to initially conducting a covered audit, an AI auditor shall do all of the following:

(1) Enroll with the agency using the mechanism established pursuant to paragraph (1) of subdivision (a) of Section 11549.82.

(2) Pay to the agency the enrollment fee set forth in paragraph (2) of subdivision (a) of Section 11549.82.

(3) Provide to the agency all of the following information:

(A) The name of the auditor.

(B) All of the following contact information:

(i) The primary physical address of the auditor, if the auditor has a physical address.

(ii) The primary internet website of the auditor, if the auditor has an internet website.

(iii) A telephone number enabling a natural person to communicate with the auditor.

(iv) An email address enabling a natural person to communicate with the auditor.

(C) The types of AI systems or models that the auditor is ~~qualified~~***enrolling*** to audit.

(D) Any relevant ~~qualifications,~~ certifications~~,~~ or accreditations,~~the auditor wishes to provide~~***, and the identities of the certifying or accrediting entities.***

(E) A written description of the auditor and the services they provide, not to exceed 200 words in length.

(F) A standard operating procedure (SOP) that describes the auditor’s procedures in sufficient detail to enable a third party to assess whether audits are conducted according to generally accepted industry best practices.

The bill also requires certain disclosures by the auditor to the auditee to ensure transparency and that the auditee is provided with the results of the audit. The author has agreed to amendments that would:

- Expand what the auditor must provide to the auditee to include the scope of the audits as well as documentation of the evidence used to arrive to the results of the audit.

- Require auditors to provide a signed document certifying the audit.

- Clarify what information an auditor must retain. As written, the bill would prohibit an auditor from conducting multiple audits of the same entity; however, this was not the intention of the bill, and, therefore, the author has accepted amendments to address this issue.

- Prohibit a covered audit from being performed by someone who was employed by the auditee in the past 12 months, in order to ensure that covered audits are performed without a conflict of interest.

The amendments are as follows:

11549.84. (a) After conducting a covered audit, an enrolled AI auditor shall provide the auditee with an audit report that contains, but is not limited to, all of the following:

(1) The scope and objective of the audit.

(~~1~~***2***) The results of the audit ***and any documentation necessary to demonstrate the basis of those results.***

(~~2~~***3***) An explanation of any steps the auditee can take to meet generally accepted industry standards appropriate to the system or model being audited.

(~~3~~***4***) An explanation of any steps the auditee can take to become compliant with state law.

(5) A statement that is signed and dated by each auditor that certifies that the covered audit was completed.

(b) An AI auditor shall not knowingly make a material misrepresentation in an audit report prepared pursuant to this subdivision.

(c) An enrolled AI auditor shall 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.

(d) 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*** ~~**a financial interest that is necessary for the performance of the audit.**~~

(e) ***(1)*** Notwithstanding Chapter 1 (commencing with Section 16600) of Part 2 of Division 7 of the Business and Professions Code, an enrolled AI auditor shall not accept employment with an auditee within 12 months of completing a covered audit of the auditee.

(2) An enrolled AI auditor shall not conduct a covered audit if the auditee employed the auditor during the 12-month period preceding the audit.

ARGUMENTS IN SUPPORT:

In support of this bill, The California Initiative for Technology & Democracy:

> Given the urgent need to increase transparency, a nascent industry has grown to provide these third-party auditing services.6 But unlike the financial auditing industry, there has been little to no regulation in the US around the standards and ethical rules governing AI auditors. Thus, like many other areas of AI policy, California must take the lead.
>
> AB 1405 tries to address this gap by requiring basic transparency and ethical standards for AI auditors. The enrollment requirement should help the public identify and judge the trustworthiness of the auditors. Moreover, the basic financial conflict of interest rules should hopefully prevent egregious manipulation of audit results. Finally, the record retention requirement can serve as support for future policy interventions to prevent harms revealed through audit and testing.
>
> To be clear, the very basic requirements AB 1405 should be the starting point for safeguards to evolve from. These basic regulations should serve to build trust in the auditing and testing results mandated in state law and empower policymakers to continue demanding transparency from companies deploying AI tools that purport to benefit Californians. Finally, these basic guardrails should not override existing rules for governing independent auditors in other contexts that set out more robust standards.

ARGUMENTS IN OPPOSITION: None on file.

REGISTERED SUPPORT / OPPOSITION:

Support

California Initiative on Technology and Democracy
Oakland Privacy
Transparency Coalition.ai

Opposition

None on file.

Analysis Prepared by: John Bennett / P. & C.P. / (916) 319-2200, Josh Tosney / P. & C.P. / (916) 319-2200