Date of Hearing: May 1, 2025
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 979 (Irwin) – As Amended April 23, 2025

SUBJECT: California Cybersecurity Integration Center: artificial intelligence

SYNOPSIS

California is home to 32 of the top 50 artificial intelligence (AI) companies, and the use cases for AI continue to expand. In September 2023, Governor Newsom issued Executive Order N-12-23 to establish a framework for assessing and deploying generative AI through pilot projects across different state agencies. This executive order laid the groundwork for what effective AI deployment could look like within the public sector. However, many AI systems have yet to demonstrate sufficient safety and resilience, posing potential risks to critical infrastructure if deployed prematurely.

In the final week of the Biden Administration, the Joint Cyber Defense Collective (JCDC), a public-private partnership, released the AI Cybersecurity Collaboration Playbook. The Playbook aims to establish best practices for information sharing regarding the risks and vulnerabilities of AI systems.

This author-sponsored bill would require the California Cybersecurity Integration Center, in coordination with the Office of Information Security, the Government Operations Agency, and relevant industry groups, to develop a California AI Cybersecurity Collaboration Playbook. Similar to its federal counterpart, this initiative would facilitate information sharing about threats to AI systems to promote safe deployment. Critically, the bill would mandate reporting mechanisms for state contractors and vendors providing AI services, requiring them to disclose known threats and vulnerabilities. It would also ensure that information can be shared confidentially between parties. This bill is supported by the Little Hoover Commission and has no opposition.

THIS BILL:

1) Requires the California Cybersecurity Integration Center to develop, in consultation with the Office of Information Security and the Government Operations Agency, a California AI Cybersecurity Collaboration Playbook to facilitate information sharing across the artificial intelligence community and to strengthen collective cyber defenses against emerging threats on or before July 1, 2026.

2) Requires the California Cybersecurity Integration Center to review federal requirements, standards, and industry best practices, including the Joint Cyber Defense Collaborative AI Cybersecurity Collaboration Playbook, and use those resources to inform the development of the California AI Cybersecurity Collaboration Playbook.

3) Requires The California AI Cybersecurity Collaboration Playbook to include mandatory mechanisms for information sharing on potential threats and vulnerabilities known to state

contractors and vendors providing AI services to a state entity identified in the California AI Cybersecurity Collaboration Playbook.

4) Permits the California AI Cybersecurity Collaboration Playbook to include voluntary mechanisms for other entities, as appropriate, to engage in information sharing on potential threats and vulnerabilities to a state entity identified in the California AI Cybersecurity Collaboration Playbook.

5) Prohibits any record or information from being disclosed to the public that is within a record of the Office of Emergency Services that is privileged, protected by copyright, or otherwise prohibited by law from being disclosed; that is exempt from disclosure to the public under express provisions of the California Public Records Act; or which based on the facts of the particular case, the public interest served by not disclosing the record clearly outweighs the public interest served by disclosure of the record.

6) Establishes that any information related to cyber threat indicators or defensive measures for a cybersecurity purpose shared in accordance with the California AI Cybersecurity Collaboration Playbook developed under this bill is confidential and prohibits that information from being transmitted or shared, except to state employees and state contractors who have been approved as necessary to receive the information and in a manner that complies with all other security requirements in the California AI Cybersecurity Collaboration Playbook.

EXISTING LAW:

1) Establishes the Cal-CSIC within the Office of Emergency Services. (Gov. Code § 8586.5 (a).)

2) Directs Cal-CSIC to serve as the central organizing hub of state government's cybersecurity activities and coordinate information sharing with local, state, and federal agencies, tribal governments, utilities and other service providers, academic institutions, including school districts, county offices of education, and charter schools, and nongovernmental organizations. (Gov. Code § 8586.5(a).)

3) Requires Cal-CSIC to provide warnings of cyberattacks to government agencies and nongovernmental partners, coordinate information sharing among these entities, assess risks to critical infrastructure and information technology networks, prioritize cyber threats and support public and private sector partners in protecting their vulnerable infrastructure and information technology networks, enable cross-sector coordination and sharing of recommended best practices and security measures. (Gov. Code § 8586.5(b).)

4) Establishes the Office of Information Security within the Department of Technology. (Gov. Code § 11549(a).)

5) Requires the Chief of the Office of Information Security to establish an information security program, and is empowered to create, update and publish policies, standards, and procedures to manage security and risk. (Gov. Code § 11549(b).)

6) Directs the Department of Technology, in consultation with the Department of General Services, and the Department of Finance, to set procedures related to the procurement of information technology. (Pub. Contr. Code § 12104(b).)

COMMENTS:

1) **Author's statement**. According to the author:

> California has a compelling interest in supporting the development and deployment of AI for the benefit of our constituents and our economy. The Legislature's role in crafting AI policy must continue to focus on creating opportunities for transparency between developers and users to build trust, acceptance, and a sense of security. By creating a California AI Cybersecurity Playbook, the state can facilitate information sharing across the artificial intelligence community and strengthen our collective cyber defenses against emerging threats.

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) **Excutive order N-12-23.** The growing use of generative AI (GenAI) is not only being pursued by private entities but also increasingly by the public sector. In September 2023, Governor Newsom signed Executive Order N-12-23, establishing a framework to study the development, use, and risks of GenAI, as well as a process for its evaluation and deployment

within state government.[1] Currently, five GenAI pilot projects are underway, addressing a range of issues, from improving road safety to enhancing healthcare facility inspections. The administration is also seeking with a Requests for Innovative Ideas (RFI2) for possible future projects. Additionally, the executive order introduced a procurement toolkit to guide state employees and officials when purchasing a GenAI tool, renewing tools that incorporate GenAI features, or encountering GenAI capabilities unexpectedly in procurement contracts.

A crucial element of deploying these new technologies is ensuring that they do not jeopardize the security of critical state infrastructure. As part of the executive order, the Government Operations Agency, the California Department of Technology (CDT), the Office of Data and Innovation, and the Governor's Office of Business and Economic Development, in collaboration with other state agencies, released a report titled "Benefits and Risks of Generative Artificial Intelligence."[2] The report highlighted that GenAI carries inherent risks and emphasized the importance of robust reporting mechanisms to ensure safety:

> As members of Cal OES's Cybersecurity Integration Center (Cal-CSIC), CDT's Office of Information Security works collaboratively with the California Highway Patrol (CHP), California Military Department (CMD), Office of Health Information Integrity, and other essential agencies on mitigating, identifying, responding to, and reporting security incidents.
>
> GenAI systems can be susceptible to unique attacks and manipulations, such as poisoning of AI training datasets, evasion attacks, and interference attacks. As with any other technology-driven threat to state security, when a state employee suspects one of these GenAI related incidents such as a GenAI- generated or -impacted incident has occurred, to the degree they're known, the employee should report it immediately for central tracking and coordination. Consistent with State Information Management Manual (SIMM) section and current practice for other technology-driven threats, it is the responsibility of the state entity Information Security Officer (ISO) or authorized user to immediately report the incident through the California Compliance and Security Incident Reporting System (Cal-CSIRS) so that further pattern analysis can be conducted for correction and safeguarding.

The Cal-CSIC's current incident reporting and information sharing apparatus focuses on cyber threat detection, reporting and response, without an explicit focus on AI or GenAI applications.[3]

4) **JCDC AI Cybersecurity Collaboration Playbook.** The Joint Cyber Defense Collective (JCDC) was established under the 2021 National Defense Authorization Act with the goal of unifying the cyber defense capabilities and actions of government and industry partners.[4] The JCDC includes participants such as Microsoft, the UK National Cyber Security Centre, and various U.S. government agencies, among many others. Through voluntary information sharing coordinated by the Cybersecurity and Infrastructure Security Agency (CISA), JCDC enables

[1] Information about Executive Order N-12-23 can be found at https://www.govops.ca.gov/generative-ai-genai-executive-order/.

[2] Report on Benefits and Risks of Generative Artificial Intelligence can be found at https://www.govops.ca.gov/generative-ai-genai-executive-order/.

[3] Cal-SCIC reporting information can be found at https://www.caloes.ca.gov/office-of-the-director/operations/homeland-security/california-cybersecurity-integration-center/.

[4] Jim Langevin and Mark Montgomery, "Making the Joint Cyber Defense Collaborative Work", *Lawfare* (Aug. 6, 2021), accessed at http://lawfaremedia.org/article/making-joint-cyber-defense-collaborative-work.

rapid, coordinated responses to cybersecurity threats with access to authoritative, real-time information.

In the final week of the Biden Administration, JCDC released the AI Cybersecurity Collaboration Playbook. The purpose of the Playbook was to:

> [F]acilitate voluntary information sharing across the AI community, including AI providers, developers, and adopters, to strengthen collective cyber defenses against emerging threats. The playbook is intended to foster operational collaboration among government, industry, and international partners and will be periodically updated to ensure adaptability to the dynamic threat landscape as AI adoption accelerates.[5]

The Playbook highlights the unique dangers that AI systems introduce due to their reliance on non-deterministic models, meaning the same input does not always produce the same output. This unpredictability leaves AI systems vulnerable to cyberattacks, such as model poisoning. In model poisoning attacks, adversaries manipulate training data or use carefully crafted inputs to introduce misleading or malicious information into models, coaxing them into generating specific or tailored responses. In some cases, attackers can poison models in ways that prevent AI systems from detecting certain types of malware, making them especially vulnerable to cyberattacks.

The Playbook also promotes the use of the Traffic Light Protocol (TLP) for information sharing. This color-coded system ensures that sensitive information is shared only with the appropriate audiences.[6] The four-color system, TLP:RED, TLP:AMBER, TLP:GREEN, and TLP:CLEAR, guides recipients on how to handle shared information, indicating how to respond to risks and whether a threat impacts privacy, management, or other critical areas of an organization. Within the Playbook framework, member organizations voluntarily share information using TLP to inform partners about potential threats.

Information sharing at this level will be critical, as AI systems are continuously tested for vulnerabilities by both ethical researchers and malicious actors. Early detection, identification, and remediation of emerging threats will rely heavily on this collaboration. As AI becomes increasingly integrated into critical infrastructure, it will be even more important for public and private sector organizations to strengthen these partnerships and ensure that AI systems are deployed securely and resiliently.

5) **What this bill would do.** This bill would require the California Cybersecurity Integration Center (Cal-CSIC), in collaboration with the Office of Information Security and the Government Operations Agency, to develop a California AI Cybersecurity Collaboration Playbook. The Playbook would facilitate the sharing of information regarding emerging risks and cybersecurity threats across the state. Cal-CSIC would be tasked with reviewing federal requirements, standards, and industry best practices, including the JCDC's AI Cybersecurity Collaboration Playbook, and using those resources to inform the development of California's Playbook. This

[5] The CISA AI Cybersecurity Playbook can be found at https://www.cisa.gov/resources-tools/resources/ai-cybersecurity-collaboration-playbook.

[6] Infromation about the TLP system and CISA can be found at https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage.

effort would bring together many of the major AI companies based in California to develop technically feasible strategies that promote the safe deployment of AI systems statewide.

However, this bill differs from the JCDC's AI Cybersecurity Collaboration Playbook by requiring mandatory reporting and information sharing for potential threats and vulnerabilities identified by state contractors and vendors providing AI services. This provision is particularly crucial as artificial intelligence becomes increasingly integrated into state infrastructure through initiatives launched under Executive Order N-12-23 and the recently announced AI initiative within the California State University system.[7] The author notes, "The state has multiple avenues in which this could be pursued, including through procurement contract language, the State Administrative Manual, or the State Information Management Manual". In addition to mandatory reporting for state-related AI services, the California AI Cybersecurity Collaboration Playbook would also include a voluntary information-sharing mechanism for threats and vulnerabilities involving non-state-connected AI systems.

To safeguard sensitive information, the bill includes provisions ensuring the confidentiality of data shared with Cal-CSIC regarding potential threats to AI systems. This includes protection for copyrighted or otherwise legally protected materials, which would be exempt from disclosure under public records requests. Finally, any information related to cyber threat indicators or defensive measures, when shared according to the Playbook, would be disclosed only to state employees and contractors who are authorized to receive it, consistent with additional security measures set forth in the Playbook.

ARGUMENTS IN SUPPORT: The Little Hoover Commission writes:

> The Little Hoover Commission supports AB 979, which would require the California Cybersecurity Integration Center to develop a California AI Cybersecurity Collaboration Playbook, in consultation with the Office of Information Security and the Government Operations Agency, to facilitate information sharing among artificial intelligence users in state government.
>
> In its 2024 report, Artificial Intelligence and California State Government, the Commission recommended broad adoption of AI for the benefit of all Californians, while also safeguarding against potential harms. Among its recommendations, the Commission called for the state to develop more robust mechanisms to anticipate and respond to AI-related threats. It also urged the state to think beyond AI and begin developing cybersecurity strategies that address emerging technological threats more broadly.
>
> AB 979 aligns with these goals by promoting cross-agency communication and coordinated planning in the face of evolving cybersecurity challenges. The development of the Cybersecurity Collaboration Playbook proposed in this bill would strengthen California's ability to implement AI safely, securely, and transparently—key values emphasized throughout the Commission's report.

REGISTERED SUPPORT / OPPOSITION:

[7] Amy DiPierro, "Cal State unveils artificial intelligence tools for students", *EdSource* (Feb. 4, 2025), accessed at https://edsource.org/2025/cal-state-unveils-artificial-intelligence-tools-for-students/726205.

Support

Little Hoover Commission

Opposition:

None on file.

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