CONCURRENCE IN SENATE AMENDMENTS
AB 979 (Irwin)
As Amended September 3, 2025
Majority vote

SUMMARY

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. 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.

Senate Amendments
Delay the implementation date until January 1, 2027.

Directs Cal-CSIC to consider how the federal government is implementing its Playbook to inform the California Playbook, as specified.

COMMENTS

1) 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.[1] 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 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.[2]

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

---

[1] 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.
[2] The CISA AI Cybersecurity Playbook can be found at https://www.cisa.gov/resources-tools/resources/ai-cybersecurity-collaboration-playbook.

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.[3] 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.

2*) 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 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.[4] 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

---

[3]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.

[4] 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.

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.

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.

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.

Arguments in Opposition

None on file.

FISCAL COMMENTS

According to the Senate Appropriations Committee:

1) The Office of Emergency Services (OES), which houses Cal-CSIC, reports total cost pressures of approximately $713,000 in the first year and $463,000 ongoing until completion of the playbook (General Fund). Costs include two limited term staff with the technical AI expertise to develop the playbook.

2) The Government Operations (GovOps) Agency anticipates costs to consult with OES to be minor and absorbable.

VOTES:

ASM PRIVACY AND CONSUMER PROTECTION: 13-0-2
YES: Bauer-Kahan, Bennett, Bryan, Flora, Irwin, Lowenthal, Ortega, Patterson, Pellerin, Petrie-Norris, Ward, Wicks, Wilson
ABS, ABST OR NV: Dixon, DeMaio

ASM APPROPRIATIONS: 14-0-1
YES: Wicks, Arambula, Calderon, Caloza, Dixon, Elhawary, Fong, Mark González, Hart, Pacheco, Pellerin, Solache, Ta, Tangipa
ABS, ABST OR NV: Sanchez

ASSEMBLY FLOOR: 78-0-1
YES: Addis, Aguiar-Curry, Ahrens, Alanis, Alvarez, Arambula, Ávila Farías, Bauer-Kahan, Bennett, Berman, Boerner, Bonta, Bryan, Calderon, Caloza, Carrillo, Castillo, Chen, Connolly, Davies, DeMaio, Dixon, Elhawary, Ellis, Flora, Fong, Gabriel, Gallagher, Garcia, Gipson, Jeff Gonzalez, Mark González, Hadwick, Haney, Harabedian, Hart, Hoover, Irwin, Jackson, Kalra, Krell, Lackey, Lee, Lowenthal, Macedo, McKinnor, Muratsuchi, Nguyen, Ortega, Pacheco, Papan, Patel, Patterson, Pellerin, Petrie-Norris, Quirk-Silva, Ramos, Ransom, Celeste Rodriguez, Michelle Rodriguez, Rogers, Blanca Rubio, Sanchez, Schiavo, Schultz, Sharp-Collins, Solache, Soria, Stefani, Ta, Tangipa, Valencia, Wallis, Ward, Wicks, Wilson, Zbur, Rivas
ABS, ABST OR NV: Bains

UPDATED

VERSION: September 3, 2025

CONSULTANT: John Bennett / P. & C.P. / (916) 319-2200 FN: 0002061