Office of Senate Floor Analyses
(916) 651-1520 Fax: (916) 327-4478

THIRD READING

Bill No: AB 979
Author: Irwin (D)
Amended: 8/29/25 in Senate
Vote: 21

SENATE GOVERNMENTAL ORG. COMMITTEE: 15-0, 6/24/25
AYES: Padilla, Archuleta, Ashby, Blakespear, Cervantes, Choi, Dahle, Hurtado, Jones, Ochoa Bogh, Richardson, Rubio, Smallwood-Cuevas, Wahab, Weber Pierson

SENATE JUDICIARY COMMITTEE: 13-0, 7/1/25
AYES: Umberg, Niello, Allen, Arreguín, Ashby, Caballero, Durazo, Laird, Stern, Valladares, Wahab, Weber Pierson, Wiener

SENATE APPROPRIATIONS COMMITTEE: 7-0, 8/29/25
AYES: Caballero, Seyarto, Cabaldon, Dahle, Grayson, Richardson, Wahab

ASSEMBLY FLOOR: 78-0, 6/2/25 - See last page for vote

SUBJECT: California Cybersecurity Integration Center: artificial intelligence

SOURCE: Author

DIGEST: This bill requires the California Cybersecurity Integration Center (Cal-CSIC) to develop a California Artificial Intelligence (AI) Cybersecurity Collaboration Playbook (Playbook) to facilitate information sharing across the AI community and to strengthen collective cyber defenses against emerging threats, as specified.

ANALYSIS:

Existing law:

1) Requires the Office of Emergency Services (OES) to establish and lead the Cal-CSIC, as specified, and requires Cal-CSIC to serve as the central organizing

hub of state government's cybersecurity activities and coordinate information sharing with specified entities, including local, state, and federal agencies.

2) Defines "artificial intelligence" 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.

This bill:

1) Requires Cal-CSIC to develop, by January 1, 2027, and in consultation with the Office of Information Security (OIS) and the Government Operations Agency (GovOps), the Playbook to facilitate information sharing across the AI community and to strengthen collective cyber defenses against emerging threats.

2) Requires Cal-CSIC 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 Playbook.

3) Requires the Playbook to include mandatory mechanisms for information sharing on potential threats and vulnerabilities known to state contractors and vendors providing AI services regarding those contracted or purchased services, to a state entity identified in the Playbook.

4) Provides that the Playbook may 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 Playbook.

5) Prohibits any record or information within a record of OES 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, as specified; or in which based on the fats of the particular case, the public interest served by not disclosing the record clearly outweighs the public interest served by disclosure of the record, from being disclosed to the public.

6) Provides that any information related to cyber threat indicators or defensive measures for a cybersecurity purpose shared in accordance with the 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 information and in a manner that complies with all other security requirements in the Playbook, as specified.

7) Includes legislative findings and declarations demonstrating the interest protected by the limitation of access to the meetings of public bodies or the writings of public officials and agencies and the need for protecting that interest, as specified.

Background

Author Statement. According to the author's office, "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."

Rapidly Evolving World of AI Technologies. The development and deployment of AI, and Generative Artificial Intelligence (GenAI), is accelerating exponentially across sectors, including within California state government. GenAI tools can produce text, images, audio, and video content by processing massive datasets. These tools offer new capabilities for public service delivery, internal operations, and constituent engagement. Unlike traditional predictive AI systems trained on narrow datasets to make recommendations, GenAI systems are designed to generate new content in response to user prompts.

California's Executive Order N-12-23 initiated a statewide effort to integrate GenAI into state operations, resulting in pilot projects, procurement toolkits, and a dedicated portal, GenAI.ca.gov. While this framework encourages adoption, it also highlights the need to address system vulnerabilities and security risks associated with GenAI tools, including model poisoning, adversarial inputs, and evasion attacks.

Executive Order N-12-23 and California's Generative AI Accountability Act. Noting California's role as a global hub for AI and the natural leader in this emerging field of technology, Governor Newsom issued EO N-12-23 in September

of 2023. In announcing the EO, Governor Newsom identified the need to deploy GenAI ethically and responsibly throughout state government, protect and prepare for potential harms, and remain the world's AI leader.

SB 896 (Dodd, Chapter 928, Statutes of 2024) known as the Generative AI (GenAI) Accountability Act codified a number of the items listed in EO N-12-23 including: requiring CDT, under the guidance of GovOps, ODI, and CalHR, to update the benefits and risks of GenAI report, as needed, to respond to significant developments; requiring OES to, as appropriate, perform a risk analysis of potential threats posed by the use of GenAI to California's critical infrastructure, including those that could lead to mass casualty events; requiring state agencies and departments to consider procurement and enterprise use opportunities in which GenAI can improve the efficiency, effectiveness, accessibility, and equity of government operations; and, requiring legal counsel for state agencies and departments to consider any potential impact of GenAI on regulatory issues under that respective agency's or department's authority and recommend necessary updates, if appropriate, as a result of this evolving technology.

Joint Cyber Defense Collaborative AI Cybersecurity Collaboration Playbook. The JCDC, established by the 2021 National Defense Authorization Act, brings together public and private sector partners to coordinate U.S. cyber defense efforts. Operated by the Cybersecurity and Infrastructure Security Agency (CISA), JCDC includes entities such as Microsoft, the UK National Cyber Security Centre, and multiple federal agencies. Through voluntary information sharing, JCDC supports real-time coordination and threat response across government and industry.

In the final days of the Biden Administration, JCDC released the AI Cybersecurity Collaboration Playbook, aimed at facilitating voluntary information exchange among AI developers, providers, and adopters. The Playbook seeks to promote operational collaboration to address AI-specific cybersecurity risks, and will be updated periodically to reflect the evolving threat landscape.

The Playbook identifies the distinct vulnerabilities of AI systems, particularly those stemming from their non-deterministic nature where identical inputs can produce different outputs. This characteristic makes AI susceptible to model poisoning attacks, where adversaries manipulate training data or introduce malicious inputs to alter model behavior. In some cases, poisoned models may even fail to detect malware, creating serious security risks.

To support responsible information exchange, the Playbook adopts the Traffic Light Protocol (TLP), a color-coded framework for designating how shared information should be handled and disclosed. TLP categories (RED, AMBER, GREEN, and CLEAR) help guide recipient organizations on how to act on shared threat data while maintaining confidentiality where necessary.

California Cybersecurity Integration Center. Cal-CSIC, within OES, is the hub of state government's cybersecurity events. Cal-CSIC coordinates information sharing at all levels of government agencies, utilities and other service providers, academic institutions, and nongovernmental organizations. Cal-CSIC's mission is to reduce the number of cyber threats and attacks in California and its focus is to respond to cyber threats and attacks that could damage the economy, its critical infrastructure, or computer networks in the state.

California AI Cybersecurity Collaboration Playbook. This bill requires Cal-CSIC, in coordination with OIS and GovOps, to develop a California AI Cybersecurity Collaboration Playbook by January 1, 2027. The purpose of the Playbook is to strengthen the state's collective cyber defenses against emerging threats associated with artificial intelligence by establishing structured mechanisms for information sharing. In developing the Playbook, Cal-CSIC must review and incorporate relevant federal standards and best practices, including the JCDC's AI Cybersecurity Collaboration Playbook.

The Playbook must include mandatory reporting requirements for state contractors and vendors that provide AI services, requiring them to share information about known threats and vulnerabilities related to those services with designated state entities. It may also include voluntary mechanisms for other organizations to participate in information sharing, where appropriate. To protect sensitive information, this bill specifies that any privileged, copyrighted, or otherwise legally protected records shall not be publicly disclosed. Additionally, any cyber threat information shared under the Playbook is considered confidential and may only be accessed by authorized state employees and contractors, in compliance with the Playbook's security protocols.

Prior/Related Legislation

SB 833 (McNerney, 2025) requires state agencies in charge of critical infrastructure that deploy AI systems to establish a human oversight mechanism to monitor its AI system's operations and to conduct annual safety and human oversight compliance assessments of its AI and automated decision systems, as

specified. This bill also requires the California Department of Technology to administer specialized training in AI safety protocols. (Pending in the Assembly Appropriations Committee)

FISCAL EFFECT: Appropriation: No Fiscal Com.: Yes Local: No

According to the Senate Appropriations Committee, 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.

GovOps anticipates costs to consult with OES to be minor and absorbable.

SUPPORT: (Verified 8/29/25)

Little Hoover Commission

OPPOSITION: (Verified 8/29/25)

None received

ARGUMENTS IN SUPPORT: In support of the bill, the Little Hoover Commission writes that, "[i]n 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."

Further, "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. If I [Chair Pedro Nava], the Commission, or our staff can be of any further assistance as this proposal moves through the legislative process, please do not hesitate to reach out."

ASSEMBLY FLOOR: 78-0, 6/2/25
AYES: 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

NO VOTE RECORDED: Bains

Prepared by: Brian Duke / G.O. / (916) 651-1530
9/2/25 18:12:13

****** END ******