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

AB 979 (Irwin)
Version: April 23, 2025
Hearing Date: July 1, 2025
Fiscal: Yes
Urgency: No
CK

SUBJECT

California Cybersecurity Integration Center: artificial intelligence

DIGEST

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

EXECUTIVE SUMMARY

Within the Office of Emergency Services (OES), Cal-CSIC stands to reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector computer networks within the state.

To address growing cyber threats and the attendant risks, the federal Cybersecurity and Infrastructure Security Agency (CISA) established a public-private partnership to "unify cyber defense capabilities" called the Joint Cyber Defense Collaborative (JCDC). In January of this year, JCDC published the AI Cybersecurity Collaboration Playbook (JCDC Playbook), which provides guidance to organizations across the AI community for sharing AI-related cybersecurity information voluntarily with CISA and other partners through JCDC.

This bill requires Cal-CSIC, in coordination with other agencies, to develop its own playbook for these same purposes and informed by the JCDC playbook and other industry standards and best practices.

The bill is author-sponsored. No timely support or opposition has been received by the Committee. This bill passed out of the Senate Governmental Organization Committee on a vote of 15 to 0.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Establishes Cal-CSIC, within the Office of Emergency Services (OES), to reduce the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, or computer networks in the state. (Gov. Code § 8586.5.)

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

3) Establishes the California Department of Technology (CDT) within the Government Operations Agency (GovOps), which is supervised by the Director of Technology. The director is the State Chief Information Officer and must report directly to the Governor on issues relating to information technology. (Gov. Code § 11545.)

4) Provides for the Office of Information Security in CDT whose purpose is to ensure the confidentiality, integrity, and availability of state systems and applications, and to promote and protect privacy as part of the development and operations of state systems and applications to ensure the trust of the residents of this state. The duties of the Office of Information Security, under the direction of the chief, are to provide direction for information security and privacy to state government agencies, departments, and offices, pursuant to Section 11549.3 of the Government Code. (Gov. Code § 11549.)

This bill:

1) Requires Cal-CSIC, on or before July 1, 2026, to develop, in consultation with the Office of Information Security and GovOps, a California 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 JCDC Playbook, and use those resources to inform the development of the California Playbook, which shall 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 California Playbook.

3) Provides that the California Playbook may include voluntary mechanisms for other entities, as appropriate, to engage in information sharing on potential threats and vulnerabilities, to the identified state entity.

4) Provides that 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; or in 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, shall not be disclosed to the public.

5) Deems, notwithstanding any other law, any information related to cyber threat indicators or defensive measures for a cybersecurity purpose shared in accordance with the California Playbook is confidential and shall not be 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 Playbook.

COMMENTS

1. Cybersecurity infrastructure in California

In order to better prepare the state for cyber attacks, Governor Brown established Cal-CSIC by executive order, Executive Order B-34-15. Eventually, in 2018, the center was codified by AB 2813 (Irwin, Ch. 768, Stats. 2018). Cal-CSIC's primary mission is to reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector computer networks in our state. It serves as the central organizing hub of the state's cybersecurity activities and coordinates information sharing with local, state, and federal agencies, tribal governments, utilities and other service providers, academic institutions, and nongovernmental organizations.

Within CDT exists the Office of Information Security. The purpose of the Office of Information Security is to ensure the confidentiality, integrity, and availability of state systems and applications, and to promote and protect privacy as part of the development and operations of state systems and applications to ensure the trust of the residents of this state. The duty of the Office of Information Security is to provide direction for information security and privacy to state government agencies, departments, and offices.

2. Creating a California Playbook to respond to emerging cyber threats

As stated, on January 14, 2025, JCDC published the AI Cybersecurity Collaboration Playbook:

> The JCDC AI Cybersecurity Collaboration Playbook facilitates 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. This playbook aims to:
>
> - Guide JCDC partners on how to voluntarily share information related to incidents and vulnerabilities associated with AI systems.
> - Outline CISA's actions upon receiving shared information.
> - Facilitate collaboration between federal agencies, private industry, international partners, and other stakeholders to raise awareness of AI cybersecurity risks and improve the resilience of AI systems.[1]

JCDC notes that while its playbook is focused on strengthening collaboration within its collaborative, it also identifies "actionable information sharing categories applicable to broader critical infrastructure stakeholders and other sharing mechanisms. CISA encourages organizations to adopt the playbook's guidance to enhance their own information-sharing practices, contributing to a unified approach to AI-related cybersecurity threats across critical infrastructure."[2]

This bill heeds this call and directs Cal-CSIC, in consultation with the Office of Information Security and GovOps, to establish a California Playbook to facilitate information sharing across the AI community and to strengthen collective cyber defenses against emerging threats. They are to review federal requirements, standards, and industry best practices, including the JCDC Playbook, and use those resources to inform the development of the California Playbook. The bill requires the establishment of mandatory mechanisms for information sharing on potential threats and vulnerabilities known to state contractors and vendors providing AI services regarding those services, to a state entity to be identified in the California Playbook. The bill also authorizes voluntary mechanisms for other entities to engage in such information sharing with the identified state entity. The bill also calls for confidentiality protections for the information so shared.

---

[1] *JCDC AI Cybersecurity Collaboration Playbook* (January 14, 2025) JCDC, https://www.cisa.gov/sites/default/files/2025-01/JCDC%20AI%20Playbook_1.pdf. All internet citations current as of June 24, 2025.

[2] *AI Cybersecurity Collaboration Playbook Fact Sheet* (January 14, 2025) JCDC, https://www.cisa.gov/sites/default/files/2025-01/JCDC%20AI%20Playbook_FACT%20SHEET.pdf.

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.

SUPPORT

None known

OPPOSITION

None known

RELATED LEGISLATION

Pending Legislation:

SB 468 (Becker, 2025) imposes a duty on a business that deploys a high-risk artificial intelligence system, or high-risk automated decision system, 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.

AB 1405 (Bauer-Kahan, 2025) establishes an enrollment process for AI auditors within GovOps. 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 for employees employed by enrolled auditors. AB 1405 is currently in this Committee and is set to be heard the same day as this bill.

Prior Legislation:

SB 1047 (Wiener, 2024) would have 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. It would have required developers to report each AI safety incident affecting a covered model to the Attorney General within 72 hours.

Governor Newsom vetoed SB 1047, stating in part:

> 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.
>
> Adaptability is critical as we race to regulate a technology still in its infancy. This will require a delicate balance. While well-intentioned, SB 1047 does not take into account whether an AI system is deployed in high-risk environments, involves critical decision-making or the use of sensitive data. Instead, the bill applies stringent standards to even the most basic functions - so long as a large system deploys it. I do not believe this is the best approach to protecting the public from real threats posed by the technology.

SB 265 (Hurtado, 2023) would have required OES to direct Cal-CSIC to prepare, and OES to submit to the Legislature on or before January 1, 2025, a strategic, multiyear outreach plan to assist critical infrastructure sectors, as defined, in their efforts to improve cybersecurity and an evaluation of options for providing grants or alternative forms of funding to improve cybersecurity preparedness. SB 265 died in the Assembly Appropriations Committee.

SB 844 (Min, Ch. 505, Stats. 2022) required Cal-CSIC to create an annual report for four years on all expenditures made by the state within a single fiscal year pursuant to the federal State and Local Cybersecurity Improvement Act.

AB 2813 (Irwin, Ch. 768, Stats. 2018) *See* Comment 1.

PRIOR VOTES:

Senate Governmental Organization Committee (Ayes 15, Noes 0)
Assembly Floor (Ayes 78, Noes 0)
Assembly Appropriations Committee (Ayes 14, Noes 0)
Assembly Privacy and Consumer Protection Committee (Ayes 13, Noes 0)
****