SENATE COMMITTEE ON APPROPRIATIONS
Senator Anna Caballero, Chair
2025 - 2026 Regular Session

AB 979 (Irwin) - California Cybersecurity Integration Center: artificial intelligence

Version: April 23, 2025
Urgency: No
Hearing Date: August 18, 2025
Policy Vote: G.O. 15 - 0, JUD. 13 - 0
Mandate: No
Consultant: Janelle Miyashiro

Bill Summary: AB 979 requires, by July 1, 2026, the California Cybersecurity Integration Center (Cal-CSIC) to develop a California Artificial Intelligence (AI) Cybersecurity Collaboration Playbook to facilitate information sharing across the AI community and to strengthen collective cyber defenses against emerging threats.

Fiscal Impact:
- The Office of Emergency Services (OES) 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.
- The Government Operations (GovOps) Agency anticipates costs to consult with OES to be minor and absorbable.

Background: 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.

Proposed Law:

- By July 1, 2026, requires Cal-CSIC, in collaboration with the Office of Information Security (OIS) and the GovOps Agency, to develop a CA AI Cybersecurity Collaboration Playbook to facilitate information sharing across the AI community and to strengthen collective cyber defenses against emerging threats.

- 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. Authorizes the playbook to include voluntary mechanisms for other entities, as appropriate, to engage in information sharing on potential threats and vulnerabilities.

- Requires Cal-CSIC to review federal requirements, standards, and industry best practices and use those resources to inform the development of the playbook.

- 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.

- 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.

- States legislative findings and declarations.

Related Legislation: AB 869 (Irwin, 2025) requires every state agency to implement Zero Trust architecture, including multifactor authentication, enterprise endpoint detection and response solutions, and robust logging practices, following uniform technology policies, standards, and procedures developed by the Chief of OIS. AB 869 is pending in this committee.

-- END --