AMENDED IN SENATE AUGUST 29, 2025

AMENDED IN ASSEMBLY APRIL 23, 2025

AMENDED IN ASSEMBLY MARCH 28, 2025

CALIFORNIA LEGISLATURE—2025–26 REGULAR SESSION

ASSEMBLY BILL No. 979

Introduced by Assembly Member Irwin

February 20, 2025

An act to amend Section 8586.5 of the Government Code, relating to technology.

LEGISLATIVE COUNSEL'S DIGEST

AB 979, as amended, Irwin. California Cybersecurity Integration Center: artificial intelligence.

Existing law requires the Office of Emergency Services to establish and lead the California Cybersecurity Integration Center. Existing law states that the center's 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 the state. Existing law requires the center 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.

This bill would require the California Cybersecurity Integration Center to develop, on or before ~~July~~ *January* 1, ~~2026,~~ *2027*, in consultation with the Office of Information Security and the Government Operations Agency, a California AI Cybersecurity Collaboration Playbook, as specified, to facilitate information sharing across the artificial intelligence community and to strengthen collective cyber defenses

against emerging threats. The bill would require the center to review federal requirements, standards, and industry best practices, as specified, and to use those resources to inform the development of the California AI Cybersecurity Collaboration Playbook. Except as specified, the bill would provide 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 is confidential and would prohibit that information from being disclosed, except as specified. The bill would also make findings and declarations related to its provisions.

Existing constitutional provisions require that a statute that limits the right of access to the meetings of public bodies or the writings of public officials and agencies be adopted with findings demonstrating the interest protected by the limitation and the need for protecting that interest.

This bill would make legislative findings to that effect.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. The Legislature finds and declares all of the following:

(a) The Joint Cyber Defense Collaborative (JCDC) is a public-private collaborative within the federal Cybersecurity and Infrastructure Security Agency that leverages authorities granted by Congress in the federal National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283) to unite the global cyber community in defense of cyberspace.

(b) On January 14, 2025, the JCDC published the JCDC AI Cybersecurity Collaboration Playbook to facilitate voluntary information sharing across the artificial intelligence (AI) community, including AI providers, developers, and adopters, to strengthen collective cyber defenses against emerging threats.

(c) The JCDC AI Cybersecurity Collaboration 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.

(d) The federal Cybersecurity Information Sharing Act of 2015 (Public Law 114-113) (CISA 2015) created protections for nonfederal entities to share cyber threat indicators and defensive measures for a cybersecurity purpose in accordance with certain requirements with the government and provides that they may do so notwithstanding any other law. These protections include the nonwaiver of privilege, protection of proprietary information, exemption from disclosure under the federal Freedom of Information Act (6 U.S.C. Sec. 552), and prohibition on use in regulatory enforcement. CISA 2015 also created protections for cyber threat indicators and defensive measures shared under its provisions with a state, tribal, or local government, including that the information shall be exempt from disclosure under local freedom of information law or similar law requiring disclosure of information or records.

SEC. 2. Section 8586.5 of the Government Code is amended to read:

8586.5. (a) The Office of Emergency Services shall establish and lead the California Cybersecurity Integration Center. The California Cybersecurity Integration Center'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 the state. The California Cybersecurity Integration Center shall 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. The California Cybersecurity Integration Center shall be composed of representatives from the following organizations:

(1) The Office of Emergency Services.
(2) The Office of Information Security.
(3) The State Threat Assessment Center.
(4) The Department of the California Highway Patrol.
(5) The Military Department.
(6) The Office of the Attorney General.
(7) The California Health and Human Services Agency.
(8) The California Utilities Emergency Association.
(9) The California State University.

(10) The University of California.
(11) The California Community Colleges.
(12) The State Department of Education.
(13) The United States Department of Homeland Security.
(14) The United States Federal Bureau of Investigation.
(15) The United States Secret Service.
(16) The United States Coast Guard.
(17) Other members as designated by the Director of Emergency Services.

(b) The California Cybersecurity Integration Center shall operate in close coordination with the California State Threat Assessment System and the United States Department of Homeland Security — National Cybersecurity and Communications Integration Center, including sharing cyber threat information that is received from utilities, academic institutions, including school districts, county offices of education, and charter schools, private companies, and other appropriate sources. The California Cybersecurity Integration Center shall 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, and support cybersecurity assessments, audits, and accountability programs that are required by state law to protect the information technology networks of California's agencies and departments.

(c) The California Cybersecurity Integration Center shall develop a statewide cybersecurity strategy, informed by recommendations from the California Task Force on Cybersecurity and in accordance with state and federal requirements, standards, and best practices. The cybersecurity strategy shall be developed to improve how cyber threats are identified, understood, and shared in order to reduce threats to California government, businesses, and consumers. The strategy shall also strengthen cyber emergency preparedness and response, standardize implementation of data protection measures, enhance digital forensics and cyber investigative capabilities, deepen expertise among California's

workforce of cybersecurity professionals, and expand cybersecurity awareness and public education.

(d) The California Cybersecurity Integration Center shall establish a Cyber Incident Response Team to serve as California's primary unit to lead cyber threat detection, reporting, and response in coordination with public and private entities across the state. This team shall also assist law enforcement agencies with primary jurisdiction for cyber-related criminal investigations and agencies responsible for advancing information security within state government. This team shall be comprised of personnel from agencies, departments, and organizations represented in the California Cybersecurity Integration Center.

(e) Information sharing by the California Cybersecurity Integration Center shall be conducted in a manner that protects the privacy and civil liberties of individuals, safeguards sensitive information, preserves business confidentiality, and enables public officials to detect, investigate, respond to, and prevent cyberattacks that threaten public health and safety, economic stability, and national security.

(f) (1) Notwithstanding Section 10231.5, the California Cybersecurity Integration Center shall create four reports that describe all expenditures made by the state within a single fiscal year pursuant to the federal State and Local Cybersecurity Improvement Act (Subtitle B of Title VI of the Infrastructure Investment and Jobs Act (Public Law 117-58), as specified in Section 665g of Title 6 of the United States Code). The reports shall be delivered to the Legislature according to the following:

(A) The first report for the 2021–22 fiscal year shall be delivered no later than December 31, 2023.

(B) The second report for the 2022–23 fiscal year shall be delivered no later than December 31, 2024.

(C) The third report for the 2023–24 fiscal year shall be delivered no later than December 31, 2025.

(D) The fourth report for the 2024–25 fiscal year shall be delivered no later than December 31, 2026.

(2) Reports to be submitted pursuant to this subdivision shall be submitted in compliance with Section 9795.

(g) (1) On or before ~~July~~ *January* 1, ~~2026,~~ *2027,* the California Cybersecurity Integration Center shall 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.

(2) The California Cybersecurity Integration Center shall 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) The California AI Cybersecurity Collaboration Playbook shall include mandatory mechanisms for information sharing on potential threats and vulnerabilities known to state contractors and vendors providing artificial intelligence services regarding those contracted or purchased services, to a state entity identified in the California AI Cybersecurity Collaboration Playbook.

(4) The California AI Cybersecurity Collaboration 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 California AI Cybersecurity Collaboration Playbook.

(5) Any record or information 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 (Division 10 (commencing with Section 7920.000) of Title 1); 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.

(6) Notwithstanding any other law, 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 subdivision 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 AI Cybersecurity Collaboration Playbook.

SEC. 3. The Legislature finds and declares that Section 2 of this act, which amends Section 8586.5 of the Government Code, imposes a limitation on the public's right of access to the meetings of public bodies or the writings of public officials and agencies within the meaning of Section 3 of Article I of the California Constitution. Pursuant to that constitutional provision, the Legislature makes the following findings to demonstrate the interest protected by this limitation and the need for protecting that interest:

The state has a very strong interest in protecting its information technology systems from intrusion because those systems contain confidential information and play a critical role in the performance of the duties of state government. Thus, information regarding the specific vulnerabilities of those systems must be protected to preclude use of that information to facilitate attacks on those systems.

O