AB-1023 California Cybersecurity Integration Center: school cybersecurity. (2023-2024)

Date Published: 10/10/2023 09:00 PM

Assembly Bill No. 1023

CHAPTER 555

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

[Approved by Governor October 08, 2023. Filed with Secretary of State October 08, 2023.]

LEGISLATIVE COUNSEL'S DIGEST

AB 1023, Papan. California Cybersecurity Integration Center: school cybersecurity.

Existing law requires the Office of Emergency Services to establish and lead the California Cybersecurity Integration Center (Cal-CSIC), to be composed of representatives from the specified organizations, with a primary mission 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.

This bill would require Cal-CSIC to include representatives from the State Department of Education.

Existing law requires Cal-CSIC to serve as the central organizing hub of the state government's cybersecurity activities and coordinate information sharing with, and share cyber threat information received from, specified public and private entities. Existing law also requires a school district, county office of education, or charter school to report any cyberattack, as defined, impacting more than 500 pupils or personnel to Cal-CSIC.

This bill would explicitly include school districts, county offices of education, and charter schools among the specified entities with which Cal-CSIC coordinates information sharing, including cyber threat information.

Vote: majority Appropriation: no Fiscal Committee: yes Local Program: no

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

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

(1) School districts, county offices of education, and charter schools are increasingly facing a broad range of cyberthreats and ransomware attacks. For many local educational agencies, it is not a matter of if they will be subject to a cybersecurity attack on their school information system, but when will one occur.

(2) Cyberattacks can render local educational agencies unable to conduct the day-to-day business of educating pupils. Successful attacks on local educational agencies have resulted in financial and learning loss, along with the exposure of private pupil data.

(3) There are over 1,000 local educational agencies in California, collecting and maintaining data related to almost 6,000,000 pupils, their families, and school employees. Much of the data local educational agencies collect and maintain is sensitive and

protected by federal and state law. Although local educational agencies take proactive steps to protect this data, they remain vulnerable to cyberattacks.

(4) Currently, the California Cybersecurity Integration Center (Cal-CSIC) serves as the central organizing hub of the state government's cybersecurity preparedness and response activities and coordinates cyber intelligence and information sharing.

(5) Due to the vast amount and great sensitivity of pupil data collected and maintained by local educational agencies, they need guidance and information to allow them to better prepare for the inevitable next cyberattack.

(b) It is, therefore, the intent of the Legislature for Cal-CSIC to provide guidance on issues of cybersecurity and preparedness to school districts, county offices of education, and charter schools.

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.