SB-844 California Cybersecurity Integration Center: cybersecurity improvement: reports. (2021-2022)

Date Published: 09/26/2022 09:00 PM

Senate Bill No. 844

CHAPTER 505

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

[Approved by Governor September 23, 2022. Filed with Secretary of State September 23, 2022.]

LEGISLATIVE COUNSEL'S DIGEST

SB 844, Min. California Cybersecurity Integration Center: cybersecurity improvement: reports.

Existing federal law, the State and Local Cybersecurity Improvement Act, establishes, within the United States Department of Homeland Security, a program to award grants to eligible entities to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state, local, or tribal governments.

Existing law establishes the California Cybersecurity Integration Center within the Office of Emergency Services, the primary mission of which is to reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or computer networks in the state. Existing law requires the center 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.

This bill would require the center to create four reports, to be delivered to the Legislature, as specified, for the 2021–22, 2022–23, 2023–24, and 2024–25 fiscal years that describe all expenditures made by the state within a single fiscal year pursuant to the federal State and Local Cybersecurity Improvement Act.

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

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

SECTION 1. 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, and nongovernmental organizations. The California Cybersecurity Integration Center shall be comprised 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 United States Department of Homeland Security.

(13) The United States Federal Bureau of Investigation.

(14) The United States Secret Service.

(15) The United States Coast Guard.

(16) 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, 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.