# AB-1306 California Cybersecurity Integration Center. (2017-2018)



Date Published: 09/16/2017 04:00 AM

ENROLLED SEPTEMBER 15, 2017

PASSED IN SENATE SEPTEMBER 14, 2017

PASSED IN ASSEMBLY SEPTEMBER 14, 2017

AMENDED IN SENATE SEPTEMBER 08, 2017

AMENDED IN SENATE SEPTEMBER 01, 2017

AMENDED IN SENATE JULY 18, 2017

AMENDED IN ASSEMBLY APRIL 06, 2017

CALIFORNIA LEGISLATURE— 2017–2018 REGULAR SESSION

## ASSEMBLY BILL NO. 1306

**Introduced by Assembly Member Obernolte**

**February 17, 2017**

An act to add Section 8586.5 to the Government Code, relating to emergency services.

## LEGISLATIVE COUNSEL'S DIGEST

AB 1306, Obernolte. California Cybersecurity Integration Center.

Existing law authorizes the Governor to make, amend, and rescind orders and regulations to implement the California Emergency Services Act. The act requires the Governor to coordinate the State Emergency Plan and those programs necessary for the mitigation of the effects of an emergency in this state. The act creates within the office of the Governor the Office of Emergency Services, which is responsible for the state's emergency and disaster response services, as specified.

By Executive order in 2015, the Governor directed the Office of Emergency Services to establish and lead the California Cybersecurity Integration Center (Cal-CSIC), with its 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 the state.

The Executive order, among other things, required that the Cal-CSIC be comprised of representatives from various entities, and that it 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.

This bill would establish in statute the Cal-CSIC within the Office of Emergency Services to develop a statewide cybersecurity strategy for California in coordination with the Cybersecurity Task Force. The bill would provide that Cal-CSIC would have the same primary mission as Cal-CSIC as created by Executive order. The bill would require Cal-CSIC to include, but not be limited to, representatives from the Office of Emergency Services, the Office of Information Security in the Department of Technology, the State Threat Assessment Center, the Department of the California Highway Patrol, the Military Department, the Office of the Attorney General, the California Health and Human Services Agency, and others.

The bill would incorporate language of the Executive order to, among other things, require Cal-CSIC to coordinate with the California State Threat Assessment System and the United States Department of Homeland Security, establish a cyber incident response team, and safeguard the privacy of individuals' sensitive information. The bill would also direct all state departments and agencies to ensure compliance with existing information security and privacy policies, promote awareness of information security standards with their workforce, and assist the California Governor's Office of Emergency Services and the Cal-CSIC.

The bill would authorize the Governor to suspend the operations of the Cal-CSIC if federal funding for its continued operation is unavailable. The bill would prohibit the Cal-CSIC from requiring private sector companies to share information but would permit voluntary sharing.
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 is added to the Government Code, to read:

**8586.5.** (a) There is established within the Governor's Office of Emergency Services the California Cybersecurity Integration Center, which shall develop a statewide cybersecurity strategy for California as set forth in subdivision (e).

(b) The primary mission of the California Cybersecurity Integration Center shall be 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.

(c) The California Governor's Office of Emergency Services shall establish and lead the California Cybersecurity Integration Center. 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 all of the following organizations:

(1) Governor's Office of Emergency Services.

(2) Department of Technology, Office of Information Security.

(3) State Threat Assessment Center.

(4) Department of the California Highway Patrol.

(5) Military Department.

(6) Office of the Attorney General.

(7) California Health and Human Services Agency.

(8) California Utilities Emergency Association.

(9) California State University.

(10) University of California.

(11) California Community Colleges.

(12) United States Department of Homeland Security.

(13) United States Federal Bureau of Investigation.

(14) United States Secret Service.

(15) United States Coast Guard.

(16) Other members as designated by the Director of the Governor's Office of Emergency Services.

(d) 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 do all of the following:

(1) Provide warnings of cyber attacks to government agencies and nongovernmental partners and coordinate information sharing among these entities.

(2) Assess risks to critical infrastructure and information technology networks.

(3) Prioritize cyber threats and support public and private sector partners in protecting their vulnerable infrastructure and information technology networks.

(4) Enable cross-sector coordination and sharing of recommended best practices and security measures.

(5) 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.

(e) 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 improve how cyber threats are identified, understood, and shared in order to reduce threats to California government, businesses, and consumers. The strategy is also intended to 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.

(f) 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 provide assistance to law enforcement agencies with primary jurisdiction for cyber-related criminal investigations and to agencies responsible for advancing information security within state government. This team shall be comprised of personnel from agencies, departments, and organizations represented on the California Cybersecurity Integration Center.

(g) 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 cyber attacks that threaten public health and safety, economic stability, and national security.

(h) All state departments and agencies shall ensure compliance with existing information security and privacy policies, promote awareness of information security standards with their workforce, and assist the California Governor's Office of Emergency Services and the California Cybersecurity Integration Center.

(i) The Governor may, by executive order, suspend the operations of the California Cybersecurity Integration Center if federal funds for its continued operation are not available. The suspension shall remain in effect only until federal funds for the operation of the California Cybersecurity Integration Center become available.

(j) In carrying out its mission, the California Cybersecurity Integration Center shall not do any of the following:

(1) Duplicate the efforts of other governmental agencies.

(2) Require involuntary information sharing by private sector entities.