SENATE COMMITTEE ON GOVERNMENTAL ORGANIZATION
Senator Bill Dodd
Chair
2021 - 2022 Regular

Bill No:	SB 892	**Hearing Date:**	4/5/2022
Author:	Hurtado		
Version:	3/22/2022 Amended		
Urgency:	No	**Fiscal:**	Yes
Consultant:	Brian Duke		

SUBJECT: Cybersecurity preparedness: food and agriculture sector and water and wastewater systems sector

DIGEST: This bill requires the California Office of Emergency Services (OES) to develop, propose, and adopt optional reporting guidelines for companies and cooperatives in the food and agriculture industry and entities in the water and wastewater systems industry if they identify a significant and verified cyber threat; and, requires OES and the California Cybersecurity Integration Center (Cal-CSIC) to prepare and submit a multiyear outreach plan to assist the food and agriculture sector and the water and wastewater sector in their efforts to improve cybersecurity and an evaluation of options for providing grants or alternative forms of funding to those sectors in their efforts to improve cybersecurity preparedness, as specified.

ANALYSIS:

Existing law:

1) The California Emergency Services Act (ESA) establishes OES, which is responsible for the state's emergency and disaster response services, as specified.

2) Requires OES to establish Cal-CSIC with the primary mission of reducing 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.

3) Requires Cal-CSIC to provide warnings of cyberattacks to government agencies and nongovernmental partners, coordinate information sharing among these entities, assess risks to critical infrastructure information networks, enable cross-sector coordination and sharing of best practices and security measures,

and support certain cybersecurity assessments, audits, and accountability programs.

4) Requires Cal-CSIC to develop a statewide cybersecurity strategy to improve how cyber threats are identified, understood, and shared in order to reduce threats to California's governments, businesses, and consumers, and to strengthen cyber emergency preparedness and response and expand cybersecurity awareness and public education.

5) The Federal, America's Water Infrastructure Act of 2018 (AWIA), requires a community water system that services a population of greater than 3,300 persons to conduct an assessment of the risks to, and resilience of, its system and to prepare or revise an emergency response plan that incorporates the findings of the assessment, as specified.

6) Specifies that any report required or requested by law to be submitted by a state or local agency to the Members of either house of the Legislature be submitted as a printed copy to the Secretary of the Senate, as an electronic copy to the Chief Clerk of the Assembly, and as an electronic or printed copy to the Legislative Counsel.

This bill:

1) Requires OES to develop and enact optional reporting guidelines applicable to companies and cooperatives in the food and agriculture industry and entities in the water and wastewater management systems industry when they identify a significant and verified cyber threat or active cyberattack. In drafting these reporting guidelines, OES shall consider, but not be limited to:

    a) A holistic view of the food and agriculture industry and the water and wastewater management systems industry, as specified.
    b) A suggested reporting timeline encouraging the affected actor to report a significant and verified cyber threat or cyberattack within 30 days of discovery.
    c) A suggested guideline that the affected actor send a report of a significant and verified cyber threat or cyberattack to any of, but not limited to: OES; Cal-CSIC; the California Department of Technology (CDT); and, the State Threat Assessment Center.
    d) Guidelines on the content for a report of a cyber threat or cyberattack, as specified.

2) Requires OES to direct Cal-CSIC to prepare a strategic, multiyear outreach plan that focuses on ways to assist the food and agriculture sector and the water and wastewater sector in their efforts to improve cybersecurity and that includes, but is not limited to, all of the following:

    a. A description of the need for greater cybersecurity outreach and assistance to the food and agriculture sector and the water and wastewater sector.
    b. The goal of the outreach plan.
    c. Methods for coordinating with other state and federal agencies, nonprofit organizations, and associations that provide cybersecurity services or resources for the food and agricultural sector and the water and wastewater sector.
    d. An estimate of the funding needed to execute the outreach plan.
    e. Potential funding sources for the funding needed by Cal-CSIC for the plan.
    f. A plan to evaluate the success of the outreach plan that includes quantifiable measures of success.

3) Requires OES to submit the outreach plan prepared pursuant to this bill to the Legislature, as specified, no later than January 1, 2024.

4) Requires OES to direct Cal-CSIC to evaluate options for providing entities in the food and agriculture sector or the water and wastewater sector with grants or alternative forms of funding to improve cybersecurity preparedness. Upon completion of the evaluation, OES shall submit a report to the Legislature, as specified, no later than January 1, 2024, that includes, but is not limited to, all of the following:

    a. A summary of the evaluation performed by Cal-CSIC.
    b. The specific grants and forms of funding for improved cybersecurity preparedness, including, but not limited to: current overall funding level and potential funding sources.
    c. Potential voluntary actions that do not require funding and assist the food and agriculture sector and the water and wastewater sector in their efforts to improve cybersecurity preparedness.

5) Specifies that this bill does not require the water and wastewater sector to submit vulnerability assessments, emergency response plans, or other related documents to the state.

6) Includes Legislative findings and declarations related to cybersecurity preparedness.

Background

Purpose of the bill. According to the author's office, "cybersecurity is an issue that continues to rise in prevalence. Without making a conscious effort to strengthen cyber defenses, entities in critical sectors put themselves and those they serve at risk of a cyberattack. This threat becomes greater when looking at two of California's most crucial sectors – its food and agriculture sector, and its water and wastewater sector. A verified cyberattack in one of these sectors has potential to be devastating. In addition to putting personal information at risk, it risks the safety and integrity of food and water that goes to millions of Californians every day. Cyberattacks also delay production, increasing food prices and hurting the consumer's wallet."

California Cybersecurity Integration Center. Initially established by Executive Order B-34-15 in 2015, Cal-CSIC was codified in statute by AB 2813 (Irwin, Chapter 557, Statutes of 2018). Cal-CSIC coordinates the state's cybersecurity activities and information sharing with federal and other state government entities. Four partners comprise the core of Cal-CSIC: OES, CDT, California Highway Patrol (CHP), and the California Military Department (CMD). OES serves as the administrative entity for Cal-CSIC, employing the Cal-CSIC Commander and Deputy Commander; CDT assesses cybersecurity policy and protocols in the event of a cyberattack; CHP looks into cybercrimes affecting the state's assets; and CMD assess potential cyber threats and vulnerabilities across state entities.

The California Department of Water Resources (DWR) works with OES on disaster preparedness, mitigation, response, and recovery activities, including from cyberattacks. WRCB's Division of Drinking Water assists with the state's drinking water resiliency efforts, including providing information on compliance with risk and readiness assessments and emergency response plans under AWIA. There are over 7,000 public drinking systems and about 900 publicly owned wastewater treatment systems in California, as well as an estimated 70,000 farms.

Critical Infrastructure Sectors. The Federal Cybersecurity and Infrastructure Agency (CISA) is one of the federal leads on national cybersecurity issues, and coordinates resilience and security efforts across critical infrastructure sectors. CISA identifies 16 critical infrastructure sectors with vial assets, networks, and systems that, if debilitated or destroyed, would have serious effects on national security, the economy, and/or public health and safety. Among the 16 identified

critical infrastructure sectors are water and wastewater systems, and food and agriculture.

Recent federal data show that cyberattacks are increasing in California. In 2020, an estimated 47,000 cyberattacks with payouts totaling $1.2 billion were reported in the state across all entities and sectors. Specifically, the author's office points to a January 2021 cyberattack by an unknown hacker in the San Francisco Bay Area. The hacker used the username and password for a former employee's account, which allowed for remote access to the network. The hacker deleted programs that the water plant used to treat drinking water. The hack wasn't discovered until the following day. Just a few weeks later, a cyberattack in Florida resulted in increasing the level of lye in public drinking water to unsafe levels for nearly 15,000 people.

America's Water Infrastructure Act of 2018. The AWIA requires community (drinking) water systems across the United States that serve more than 3,300 people to certify their completion of risk and readiness assessments and emergency response plans to the EPA. Risk and readiness assessments evaluate the risks to, and resilience of, community water systems across several categories, including the security of information technology (IT) and operational technology (OT) systems used to convey water. Emergency response plans incorporate findings from the risk and readiness assessments and identify resources and strategies to improve the security of the community water systems, including their cybersecurity. These plans also identify mitigation measures in the event of, as relevant to this memorandum, a cyberattack that affects the safety and/or supply of drinking water, such as the identification of alternative drinking water options and operation of physical infrastructure without the use of IT or OT systems. Public data on these certifications is available on the EPA's website.

State Threat Assessment Center. The State Threat Assessment Center is California's state primary fusion center, as designed by the Governor of California, and is operated by the CHP, OES, and the Department of Justice (DOJ). The center serves as California's information sharing clearinghouse of strategic threat analysis and situational awareness reporting to statewide leadership and the public safety community in support of efforts to prevent, prepare for, mitigate and respond to all crimes and hazards impacting California citizens and critical infrastructure.

This bill requires OES to develop and enact *optional* reporting guidelines applicable to companies and cooperatives in the food and agriculture industry and entities in the water and wastewater management system industry when they identify a significant and verified cyber threat or active cyberattack. In drafting

these guidelines, OES must consider, but not be limited to: a holistic view of the food and agriculture industry and the water and wastewaters systems industry; suggested reporting timelines; suggested guidelines for reporting to various identified state agencies; and, guidelines on the content and details on the structure of the cyber threat or attack.

Additionally, this bill directs Cal-CSIC to prepare a strategic, multiyear outreach plan that focuses on ways to assist the food and agriculture sector and the water and wastewater sector in their efforts to improve cybersecurity. This bill requires that the outreach plan be reported to the Legislature no later than January 1, 2024.

Finally, this bill requires Cal-CSIC to evaluate options for providing entities in the food and agriculture sector or the water and wastewater sector with grants or alternative forms of funding to improve cybersecurity preparedness. This review is also due to the Legislature in the form of a report no later than January 1, 2024, and must include, among other things: a summary of the evaluation; the specific grants and forms of funding for improved cybersecurity preparedness including current overall funding level and potential funding sources; and, potential voluntary actions that do not require funding and assist the food and agriculture sector and the water and wastewater sector in their efforts to improve cybersecurity preparedness.

Prior/Related Legislation

AB 2135 (Irwin, 2022) requires state agencies, as defined, to adopt and implement information security and privacy policies, standards, and procedures based upon specified standards. (Pending in the Assembly Privacy and Consumer Protection Committee)

AB 2355 (Salas, 2022) requires local educational agencies to report any cyberattack to Cal-CSIC, as specified. (Pending in the Assembly Education Committee)

SB 468 (Dodd, 2021) adds "electromagnetic pulse attack" to the list of conditions constituting a state of emergency and a local emergency. (Pending referral in the Assembly Rules Committee)

AB 581 (Irwin, 2021) requires state agencies, as defined, to review and implement specified National Institute of Standards and Technology guidelines for, among other things, reporting, coordinating, publishing, and receiving information about a security vulnerability relating to information systems and the resolution thereof, as specified. (Pending referral in the Senate Rules Committee)

AB 1352 (Chau, Chapter 593, Statutes of 2021) authorizes the CMD, at the request of a local education agency, and in consultation with Cal-CSIC, to perform an independent security assessment of the local education agencies, as specified.

SB 532 (Dodd, Chapter 557, Statutes of 2018) included "cyberterrorism" within the conditions constituting a state of emergency and a local emergency.

AB 2813 (Irwin, Chapter 768, Statutes of 2018) established in statute Cal-CSIC within OES, the primary mission of which is the same as the Cal-CSIC as created by the previous executive order.

FISCAL EFFECT: Appropriation: No Fiscal Com.: Yes Local: No

SUPPORT:

None received

OPPOSITION:

Agricultural Council
California Farm Bureau Federation
California Municipal Utilities Association
California Special Districts Association
Western Growers Association

ARGUMENTS IN OPPOSITION: The Western Growers Association, California Farm Bureau Federation, and Agricultural Council jointly write that, "SB 892 creates suggested optional guidelines that potentially apply to the entire agriculture industry. In no instance has any single state experienced a coordinated cyberattack across farmers and ranchers of all sizes at such scale as to cause food system disruption or a risk to public health. Even as amended, SB 892 casts a very wide net across all of California's food supply chain to ensure food safety when the few cyberattacks in recent years have been ransom requests for financial gain. In our discussions with Senator Hurtado's office, it is unclear what type of systems would come under cyberattack on-farm, particularly on small and mid-sized farms, that would disrupt and produce unsafe conditions for the public further down the supply chain."