
UNFINISHED BUSINESS

Bill No: SB 892
Author: Hurtado (D), et al.
Amended: 8/15/22
Vote: 21

SENATE GOVERNMENTAL ORG. COMMITTEE: 9-0, 4/5/22

AYES: Dodd, Allen, Archuleta, Becker, Glazer, Hueso, Kamlager, Portantino, Rubio

NO VOTE RECORDED: Nielsen, Borgeas, Bradford, Jones, Melendez, Wilk

SENATE APPROPRIATIONS COMMITTEE: 5-2, 5/19/22

AYES: Portantino, Bradford, Kamlager, Laird, Wieckowski

NOES: Bates, Jones

SENATE FLOOR: 25-7, 5/24/22

AYES: Allen, Atkins, Becker, Bradford, Cortese, Dodd, Durazo, Eggman, Glazer, Gonzalez, Hueso, Hurtado, Laird, Leyva, Limón, McGuire, Min, Pan, Portantino, Roth, Rubio, Stern, Umberg, Wieckowski, Wiener

NOES: Bates, Dahle, Grove, Jones, Nielsen, Ochoa Bogh, Wilk

NO VOTE RECORDED: Archuleta, Borgeas, Caballero, Hertzberg, Kamlager, Melendez, Newman, Skinner

ASSEMBLY FLOOR: 75-0, 8/23/22 - See last page for vote

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

SOURCE: Author

DIGEST: This bill requires the California Office of Emergency Services (OES) to direct the California Cybersecurity Integration Center (Cal-CSIC) to prepare and submit a strategic, multiyear outreach plan to assist the food and agriculture sector and the water and wastewater sector in their efforts to improve cybersecurity, as specified.

Assembly Amendments delete the requirement that OES develop and adopt optional reporting guidelines applicable to companies and cooperatives in the food and agriculture industry and entities in the water and wastewater systems industry, as specified, and delete the cyberattack or cyber threat reporting requirement, as specified.

ANALYSIS:

Existing law:

- 1) Establishes OES, pursuant to the California Emergency Services Act (ESA), 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) 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 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.
- 2) Requires OES to submit the outreach plan to the Legislature no later than January 1, 2024, as specified.
- 3) 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, as specified. Upon completion of the evaluation, OES shall submit a report to the Legislature 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.
- 4) Makes related legislative findings and declarations.

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, as well."

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, the California Department of Technology (CDT), the 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.

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 vital 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.

This bill requires 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 OES to submit the outreach plan to the Legislature by January 1, 2024. Further, 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.

Related/Prior 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 on the Senate Floor)

AB 2355 (Salas, 2022) requires local educational agencies to report any cyberattack to Cal-CSIC, as specified. (Pending on the Senate Floor)

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

According to the Assembly Appropriations Committee, one-time costs of an unknown amount to OES to develop cybersecurity outreach plans for the specified industries. (General Fund)

SUPPORT: (Verified 8/22/22)

California Water Association
California Water Service

OPPOSITION: (Verified 8/22/22)

None received

ARGUMENTS IN SUPPORT: In support of this bill, the California Water Association writes that, “[p]ortions of California’s water and wastewater sector suffer from a significant lack of cybersecurity preparedness. This lack of defense opens these life-sustaining systems to cyberattacks, including phishing attempts and ransomware. These threats ultimately threaten the health and safety of Californians who rely on these sectors. Just last year, a hacker deleted several of the programs needed to operate a wastewater treatment plant here in California. While the threat was addressed before damage was done, lack of preparedness could result in a much different outcome.”

ASSEMBLY FLOOR: 75-0, 8/23/22

AYES: Aguiar-Curry, Alvarez, Arambula, Bauer-Kahan, Bennett, Berman, Bloom, Boerner Horvath, Mia Bonta, Bryan, Calderon, Carrillo, Cervantes, Chen, Choi, Cooley, Cooper, Cunningham, Megan Dahle, Daly, Mike Fong, Fong, Friedman, Gabriel, Cristina Garcia, Eduardo Garcia, Gipson, Grayson, Haney, Holden, Irwin, Jones-Sawyer, Kalra, Kiley, Lackey, Lee, Levine, Low, Maienschein, Mathis, Mayes, McCarty, McKinnor, Medina, Mullin, Muratsuchi, Nazarian, Nguyen, O'Donnell, Patterson, Petrie-Norris, Quirk, Quirk-Silva, Ramos, Reyes, Luz Rivas, Robert Rivas, Rodriguez, Blanca Rubio, Salas, Santiago, Seyarto, Smith, Stone, Ting, Valladares, Villapudua, Voepel, Waldron, Ward, Akilah Weber, Wicks, Wilson, Wood, Rendon
NO VOTE RECORDED: Bigelow, Davies, Flora, Gallagher, Gray

Prepared by: Brian Duke / G.O. / (916) 651-1530
8/23/22 15:12:09

**** **END** ****