SENATE THIRD READING
SB 892 (Hurtado)
As Amended August 15, 2022
Majority vote

## SUMMARY

Requires the California Office of Emergency Services (Cal OES) to direct the California Cybersecurity Integration Center (Cal-CSIC) to better educate and prepare companies and cooperatives in the food and agriculture industry and entities in the water and wastewater management system industry for cyber threats and cyberattacks, as specified.

**Major Provisions**

1) Requires Cal OES to direct 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.

2) Makes related findings and declarations, such these sectors can help the State's cybersecurity preparedness by reporting significant and verified cyber threats or attacks.

## COMMENTS

*California Cybersecurity Integration Center*: In 2015, a Governor Brown Executive Order created the Cal-CSIC and, in 2018, Cal-CSIC was established in statute by AB 2813 (Irwin), Chapter 768, Statutes of 2018. Under the umbrella of Cal OES, the California Cybersecurity Integration Center serves as the central organizing hub of state government's cybersecurity activities and coordinates information sharing among stakeholders that include local, state, and federal agencies, tribal governments, utilities and other service providers, academic institutions, and nongovernmental organizations. It is co-located at the California State Threat Assessment Center with the 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.

To foster statutorily mandated coordination, Cal-CSIC is required to have 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 more. Additionally, Cal-CSIC coordinates directly with the California State Threat Assessment Center and the United States Department of Homeland Security.

Cal-CSIC is also tasked with developing a statewide cybersecurity strategy, in accordance with state and federal standards, to improve how cyber threats are identified, understood, and shared in order to reduce threats to the California government, businesses, and consumers; providing warnings of cyberattacks to government agencies and nongovernmental partners; establishing a cyber-incident response team; safeguarding the privacy of individual's sensitive information; assessing risks to critical infrastructure and information technology networks; supporting

cybersecurity assessments, audits, and accountability programs; and collecting and sharing cyber threat information with relevant parties.

*Ongoing Cyber Threats to U.S. Water and Wastewater Systems*: On October 14, 2021, a joint advisory was released by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Agency (CISA), the Environmental Protection Agency (EPA), and the National Security Agency (NSA) to highlight ongoing malicious cyber activity aimed targeting the water and wastewater systems.

*Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons*: According to an FBI flash alert issued on April 20, 2022, "ransomware actors may be more likely to attack agricultural cooperatives during critical planting and harvest seasons" like the fall and early spring. The FBI warning is one of many issued by the U.S. government over the past year regarding the cybersecurity of the agriculture industry and the rising risk of ransomware attacks. This latest warning cites several instances in which different agriculture sector organizations across the country have been targeted by ransomware in both the planting and harvesting seasons.

The FBI alert on ransomware threats to the agriculture industry coincided with another warning from the U.S. Government. A joint security advisory from the Cybersecurity and Infrastructure Security Agency, the National Security Agency and Department of Justice announced critical infrastructure organizations could see "increased malicious cyber activity" from Russian threat groups.

**According to the Author**
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.

**Arguments in Support**
The California Water Service writes in support, "SB 892 establishes voluntary reporting requirements for the water and wastewater sector in the event of verified cyber threat or cyberattack. SB 892 also encourages the state's cybersecurity agencies to strengthen California's defenses against cyberattacks. While modest, these provisions will do much to help protect against emerging threats faced by the water and wastewater sector.
Cybersecurity is absolutely critical to water suppliers as we provide the only public utility service that is consumed by our customers. Ensuring the safety of the life-sustaining product we provide to our customers is vital; we can't get it wrong."

**Arguments in Opposition**
No opposition on file.

## FISCAL COMMENTS

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)"

## VOTES

**SENATE FLOOR: 25-7-8**
**YES:** 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
**NO:** Bates, Dahle, Grove, Jones, Nielsen, Ochoa Bogh, Wilk
**ABS, ABST OR NV:** Archuleta, Borgeas, Caballero, Hertzberg, Kamlager, Melendez, Newman, Skinner

**ASM EMERGENCY MANAGEMENT: 6-0-1**
**YES:** Rodriguez, Seyarto, Calderon, Gray, Waldron, Ward
**ABS, ABST OR NV:** Aguiar-Curry

**ASM APPROPRIATIONS: 12-0-4**
**YES:** Holden, Bryan, Calderon, Arambula, Mike Fong, Gabriel, Eduardo Garcia, Levine, Quirk, Robert Rivas, Akilah Weber, McCarty
**ABS, ABST OR NV:** Bigelow, Megan Dahle, Davies, Fong

## UPDATED

VERSION: August 15, 2022

CONSULTANT: Mike Dayton / E.M. / (916) 319-3802 FN: 0003570