Date of Hearing: August 3, 2022

ASSEMBLY COMMITTEE ON APPROPRIATIONS
Chris Holden, Chair
SB 892 (Hurtado) – As Amended June 16, 2022

Policy Committee: Emergency Management Vote: 6 - 0

Urgency: No State Mandated Local Program: No Reimbursable: No

SUMMARY:

This bill requires the Office of Emergency Services (OES) to develop and adopt optional reporting guidelines applicable to companies and cooperatives in the food and agriculture industry and entities in the water and wastewater industry regarding identification of a significant and verified cyberattack. Any report of a cyberattack or cyber threat submitted pursuant to the developed guidelines is confidential and not subject to disclosure as a public record. This bill also requires OES to direct the California Cybersecurity Integration Center (Cal-CSIC) to prepare, by January 1, 2024, a multi-year outreach plan to assist the agriculture and water industries in efforts to improve cybersecurity and options for providing grants and other support to improve cybersecurity preparedness.

FISCAL EFFECT:

Costs of approximately $2.8 million in the first year and approximately $3.0 million ongoing to OES for seven additional staff positions, training and information technology tools to develop cybersecurity guidelines and outreach plans for the specified industries. (General Fund)

COMMENTS:

1) **Purpose.** According to the author:

> [The threat of a cyberattack] 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.
>
> SB 892 address cybersecurity in these sectors by requesting that they both prioritize strong cybersecurity.

2) **Support and Opposition.** This bill is supported by some public water utilities, but is opposed, unless amended, by some agriculture groups. In support, the California Water Association explains, "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." In opposition, the California Farm Bureau Federation, Western Growers Association and Agricultural Council of California jointly argue, "adding a new regulation that requires every single farm in the state to report about cyber incidents is an overreach, and in light of federal legislation, creates the potential for additional costs, confusion, and non-compliance."

3) **Cal-CSIC.** Under the umbrella of OES, Cal-CSIC serves as the central organizing hub of state government's cybersecurity activities and coordinates information sharing among stakeholders, including local, state and federal agencies, tribal governments, utilities and other service providers, academic institutions and nongovernmental organizations. Cal-CSIC 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, critical infrastructure or public and private sector computer networks.

4) **Recent Federal Efforts.** The federal State and Local Cybersecurity Improvement Act (Improvement Act) included in the $1.2 trillion Infrastructure Investment and Jobs Act bill package signed by President Biden in November 2021 authorized a new $1 billion grant program to improve cybersecurity at the state, territorial, local and tribal level, allocated over four years by the Federal Emergency Management Agency. The state must first submit a cybersecurity plan to be eligible for funding and distribute 80% of awarded funds to local governments. Awardees must generally match a percentage of funds, with the match percentage growing gradually each year.

   Additionally, the federal Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Reporting Act) was included in an omnibus appropriations bill following high-profile cyberattacks on critical infrastructure providers and growing concerns of retaliatory cyberattacks related to Russia's invasion of Ukraine. Owners and operators of critical infrastructure must report certain cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) at the U.S. Department of Homeland Security within 72 hours and report ransomware payments within 24 hours. The new reporting obligations do not take effect until the CISA director promulgates regulations, but critical infrastructure will likely include the food and agriculture and water and wastewater industries, amongst many others, as the Federal Bureau of Investigation has highlighted ongoing ransomware attacks on both industries. This bill requires OES to adopt separate, optional reporting guidelines for both industries and requires Cal-CSIC to develop a plan to help both industries improve cybersecurity.

5) **Related Legislation.** SB 844 (Min) requires Cal-CSIC to create four reports to the Legislature for fiscal years 2021-22, 2022-23, 2023-24 and 2024-25 describing all expenditures made by the state pursuant to the Improvement Act. SB 844 is pending hearing by this committee.

Analysis Prepared by: Irene Ho / APPR. / (916) 319-2081