Date of Hearing: June 27, 2022

ASSEMBLY COMMITTEE ON EMERGENCY MANAGEMENT
Freddie Rodriguez, Chair
SB 892 (Hurtado) – As Amended June 16, 2022

SENATE VOTE: 25-7

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

SUMMARY: Requires the California Office of Emergency Services (Cal OES) to develop optional guidelines for companies and cooperatives in the food and agriculture industry and for entities in the water and wastewater management system industry to report cyber threats or cyberattacks, as specified. Specifically, **this bill**:

1) Requires Cal 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.

2) Requires Cal 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.

3) Requires a report of a cyberattack or cyber threat submitted pursuant to the optional guidelines be confidential and would prohibit disclosure of such report as a public record.

EXISTING LAW:

1) Establishes the Cal OES within the office of the Governor and makes Cal OES responsible for the state's emergency and disaster response services for natural, technological, or manmade disasters and emergencies.

2) Authorizes the Governor to proclaim a state of emergency and local officials and local governments to proclaim a local emergency, when specified conditions of disaster or extreme peril to the safety of persons and property exist, and authorizes the Governor or the appropriate local government to exercise certain powers in response to that emergency.

3) Establishes the Cal-CSIC within Cal OES to, among other things, reduce the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or computer networks in the state; serve as the central organizing hub of state government's cybersecurity activities; and to coordinate information sharing with relevant stakeholders.

4) Requires the Cal-CISC to develop a statewide cybersecurity strategy to improve how cyber threats are identified, understood, and shared in order to reduce threats and to

strengthen cyber emergency preparedness and expand cybersecurity awareness and public education.

5) Establishes, within the United States Department of Homeland Security, a program to award grants to eligible entities to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state, local, or tribal governments.

FISCAL EFFECT: According to the Senate Committee on Appropriations, "Cal OES estimates first year costs of approximately $2,789,000 and ongoing annual costs of approximately $2,996,000 (General Fund). Costs include expenses for additional staff, training, tools, and other software."

COMMENTS:

Purpose of the bill: 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."

"SB 892 addresses cybersecurity in these sectors by requesting that they both prioritize strong cybersecurity. By encouraging both food and agriculture companies, and water and wastewater sector entities to disclose verified cyber threats and cyberattacks, SB 892 emphasizes that these incidents should not be swept away without receiving the attention they deserve. SB 892 also allows California's Cybersecurity Integration Center to explore avenues of increasing cybersecurity outreach and finding potential areas of funding to ensure that these sectors receive the support they need from the State to build out their cyber defenses," concludes the author.

California Emergency Services Act: The California Emergency Services Act (ESA) was enacted in 1970, and established Cal OES within the Governor's Office. The ESA gives the Governor authority to proclaim a state of emergency in an area affected or likely to be affected when: conditions of disaster or extreme peril exist; the Governor is requested to do so upon request from a designated local government official; or the Governor finds that local authority is inadequate to cope with the emergency. Local governments may also issue local emergency proclamations, which is a prerequisite for requesting the Governor's Proclamation of a State of Emergency.

Emergency Preparedness and Response: Cal OES is responsible for addressing natural, technological, or manmade disasters and emergencies, and preparing the State to prevent, respond to, quickly recover from, and mitigate the effects of both intentional and natural disasters. As part of their overall preparedness mission, Cal OES is required to develop a State Emergency Plan (SEP), State Hazard Mitigation Plan (SHMP), and maintains Standardized Emergency Management System (SEMS) and the Emergency Management Mutual Aid System (EMMA). Cal OES, in coordination with FEMA and local partners, has developed four Catastrophic Plans to augment the State Emergency Plan.

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.

Federal Cyber Incident Report for Critical Infrastructure Act: On March 15, 2022, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act into law, which was included in an omnibus appropriations bill. Against the backdrop of high-profile cyberattacks on critical infrastructure providers and growing concerns of retaliatory cyberattacks relating to Russia's invasion of Ukraine, the House approved the bipartisan legislation on March 9 and the Senate unanimously approved the legislation on March 11 after failing to pass similar legislation in recent years.

The Act creates two new reporting obligations on owners and operators of critical infrastructure: (1) an obligation to report certain cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) within 72 hours, and (2) an obligation to report ransomware payments within 24 hours.

The new reporting obligations will not take effect until the Director of CISA promulgates implementing regulations, including "clear description[s] of the types of entities that constitute covered entities." The Act does provide guideposts for which entities may be covered and refers to the Presidential Policy Directive 21 from 2013, which deems the following sectors as critical infrastructure: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services, energy; financial services; food and agriculture;

government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

America's Water Infrastructure Act of 2018: The AWIA requires each community (drinking) water system across the United States that serves 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.

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. The advisory details the ongoing cyber threats and noted the following water and wastewater systems sector cyber intrusions associated with insider threats, from current or former employees who maintain improperly active credentials, and ransomware attacks:

- In August 2021, malicious cyber actors used Ghost variant ransomware against a California-based WWS facility. The ransomware variant had been in the system for about a month and was discovered when three supervisory control and data acquisition (SCADA) servers displayed a ransomware message.
- In July 2021, cyber actors used remote access to introduce ZuCaNo ransomware onto a Maine-based WWS facility's wastewater SCADA computer. The treatment system was run manually until the SCADA computer was restored using local control and more frequent operator rounds.
- In March 2021, cyber actors used an unknown ransomware variant against a Nevada-based WWS facility. The ransomware affected the victim's SCADA system and backup systems. The SCADA system provides visibility and monitoring but is not a full industrial control system (ICS).
- In September 2020, personnel at a New Jersey-based WWS facility discovered potential Makop ransomware had compromised files within their system.
- In March 2019, a former employee at Kansas-based WWS facility unsuccessfully attempted to threaten drinking water safety by using his user credentials, which had not been revoked at the time of his resignation, to remotely access a facility computer.

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.

According the FBI's flash alert, "Since 2021, multiple agricultural cooperatives have been impacted by a variety of ransomware variants. Initial intrusion vectors included known, but unpatched, common vulnerabilities and exploits, as well as secondary infections from the exploitation of shared network resources or compromise of managed services." The following ransomware attack incidents were highlighted:

- In March 2022, a multi-state grain company suffered a Lockbit 2.0 ransomware attack. In addition to grain processing, the company provides seed, fertilizer, and logistics services, which are critical during the spring planting season.
- In February 2022, a company providing feed milling and other agricultural services reported two instances in which an unauthorized actor gained access to some of its systems and may have attempted to initiate a ransomware attack. The attempts were detected and stopped before encryption occurred.
- Between 15 September and 6 October 2021, six grain cooperatives experienced ransomware attacks. A variety of ransomware variants were used, including Conti, BlackMatter, Suncrypt, Sodinokibi, and BlackByte. Some targeted entities had to completely halt production while others lost administrative functions.
- In July 2021, a business management software company found malicious activity on its network, which was later identified as HelloKitty/Five Hands ransomware. The threat actor demanded $30 million USD ransom. The ransomware attack on the company led to secondary ransomware infections on a number of its clients, which included several agricultural cooperatives.

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.

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 cyber attacks. 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."

The California Water Association writes in support, "Portions 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."

Oppose unless amended arguments: The Western Growers Association, the California Farm Bureau Federation and Agricultural Council of California write, "The vast majority of California farmers are not yet aware of how cyber-threats on the farm could impact public safety, nor do they have the technical expertise to maintain a cyber security tracking system to capture and log events and report those to the state. Our proposed amendments to SB 892 will help the state educate the industry about these risks, and help provide farmers and ranchers with technical expertise to implement tools to ensure necessary safety on the farm. These amendments will increase the likelihood that farmers will report cyber-attacks to the state by educating the industry on the risks, and importance of reporting."

Related Legislation:

SB 844 (Min, 2022) requires the California Cybersecurity Integration Center (Cal-CSIC) to create an annual report for four years on all expenditures made by the state within a single fiscal year pursuant to the federal State and Local Cybersecurity Improvement Act. (Pending in the Assembly Committee on Emergency Management)

SB 1001 (Min, 2022) requires Cal-CSIC to submit a report to the Legislature on the feasibility and benefits of requiring credit reporting bureaus and lenders to implement new information security tactics that protect consumers from financial fraud, as specified. (Pending in the Assembly Appropriations Committee)

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

AB 2813 (Irwin, Chapter 768, Statutes of 2018) established Cal-CSIC in statute, as specified.

REGISTERED SUPPORT / OPPOSITION:

Support

California Water Association
California Water Service

Oppose Unless Amended

Western Growers Association
California Farm Bureau Federation
Agricultural Council of California

Analysis Prepared by: Mike Dayton / E.M. / (916) 319-3802