STATE OF CALIFORNIA
Budget Change Proposal - Cover Sheet
DF-46 (REV 10/20)

Fiscal Year	Business Unit	Department	Priority No.
2023-24	0690	Office of Emergency Services	

Budget Request Name	Program	Subprogram
0690-031-BCP-2023-GB	0380 – Emergency Management Services	

Budget Request Description
Food and Agriculture Sector and Water and Wastewater Sector Cybersecurity (SB 892)

Budget Request Summary
The Office of Emergency Services requests $531,000 General Fund in 2023-24 and $280,000 in 2024-25 to implement Chapter 820, Statutes of 2022 (SB 892).

Requires Legislation	Code Section(s) to be Added/Amended/Repealed
☐ Yes ☒ No	

Does this BCP contain information technology (IT) components? ☒ Yes ☐ No *If yes, departmental Chief Information Officer must sign.*	Department CIO	Date

For IT requests, specify the project number, the most recent project approval document (FSR, SPR, S1BA, S2AA, S3SD, S4PRA), and the approval date.

Project No. **Project Approval Document:**

Approval Date:

If proposal affects another department, does other department concur with proposal? ☐ Yes ☐ No
Attach comments of affected department, signed and dated by the department director or designee.

Prepared By	Date	Reviewed By	Date
Budget Office	10/6/2022		
Department Director	**Date**	**Agency Secretary**	**Date**

Department of Finance Use Only

Additional Review: ☐ Capital Outlay ☐ ITCU ☐ FSCU ☐ OSAE ☐ Dept. of Technology

PPBA	Date submitted to the Legislature
Stephen Benson	1/10/2023

A. Budget Request Summary

The Office of Emergency Services (Cal OES) requests $531,000 General Fund in 2023-24 and $280,000 in 2024-25 to implement Chapter 820, Statutes of 2022 (SB 892).

B. Background/History

Chapter 768, Statutes of 2018 (AB 2813) codified the California Cyber Security Integration Center (Cal-CSIC) in Government Code Section 8586.5 and set forth its composition and responsibilities. By statute, the Cal-CSIC is designed to include representatives from Cal OES, the Department of Technology, the State Threat Assessment Center (STA), the California Highway Patrol, the Military Department, the Office of the Attorney General, and the California Health and Human Services Agency, as well as other stakeholders from state and federal governments and the private sector. The statute further requires the Cal-CSIC to coordinate with the California State Threat Assessment Center (STAC) and the United States Department of Homeland Security (DHS), to establish a cyber-incident response team and safeguard the privacy of individuals' sensitive information.

Cal-CSIC serves as the central organizing hub of state government's cybersecurity activities and coordinates information sharing with local, state, and federal agencies, tribal governments, utilities and other service providers, academic institutions, and nongovernmental organizations. These services include program elements such as overarching cybersecurity strategy, intelligence analysis, information sharing, and incident response. States and local municipalities nationwide are being barraged by cyberattacks and frequent probing, where attackers are seeking monetary gain, opportunities to disrupt operations, or to cause permanent damage and destruction to information systems and sensitive data on employees and citizens alike.

It is important that all the above-mentioned services, as well as others not listed, are integrated through a common set of security principles and best practices that establish a unity of effort through the Cal-CSIC.

SB 892 requires Cal OES and the 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 improving cybersecurity and an analysis of grants or alternative funding sources to improve cybersecurity preparedness. Specifically, SB 892 requires the Cal-CSIC to:

- Provide descriptions of the need for greater cybersecurity outreach and assistance to the food and agriculture sector and the water and wastewater sector
- Provide the goals of the outreach plan
- Coordinate methods 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
- Provide an estimate of the funding needed to execute the outreach plan
- Identify potential funding sources for the funding needed; and
- Establish a plan to evaluate the success of the outreach plan that includes quantifiable measures of success

C. State Level Consideration

This proposal is consistent with Cal OES' mission to protect lives and property, build capabilities, and support communities for a resilient California. Additionally, the Cal OES Strategic Plan contains the following goals:

Goal 1: Anticipate and enhance prevention and detection capabilities to protect our state from all hazards and threats.

Goal 2: Strengthen California's ability to plan, prepare for, and provide resources to mitigate the impacts of disasters, emergencies, crimes, and terrorist events.

Goal 3: Effectively respond to and recover from both human-caused and natural disasters.

Goal 4: Enhance the administration and delivery of all state and federal funding and maintain fiscal and program integrity.

Goal 5: Develop a united and innovative workforce that is trained, experienced, knowledgeable, and ready to adapt and respond.

Goal 6: Strengthen capabilities in public safety communication services and technology enhancements.

The goals and objectives of the California Homeland Security Strategy serve as the framework for prioritizing and developing statewide homeland security capabilities over the next three years. This proposal supports the following goals:

Goal 1: Enhance Information Collection, Analysis, and Sharing, in Support of Public Safety Operations across California

Goal 2: Protect Critical Infrastructure and key Resources from All Threats and Hazards

Goal 3: Strengthen Security and Preparedness across Cyberspace

Goal 4: Strengthen Communications Capabilities through Planning, Governance, Technology, and Equipment Goal 5: Enhance Incident Recovery Capabilities

In 2021, CDT and the Cal-CSIC jointly developed Cal-Secure, a multi-year cybersecurity roadmap for California. Cal-Secure was approved and endorsed by the Governor, and it follows the establishment of the California Homeland Security Strategy (specifically, the goal of Strengthen Security and Preparedness across Cyberspace) and the State Technology Strategic Plan: Vision 2023. Cal-Secure is broken into three roadmap categories − people, process, and technology, which the executive branch will focus on throughout the next five years to improve its cybersecurity maturity and identify and manage risks to the state. This plan outlines success measures that the state will achieve upon completion of the Cal-Secure objectives. Each category is equally important to achieve to ensure the success of the five-year plan.

D. Justification

The Cal-CSIC is currently operating under a three-year funding commitment, set to expire on June 30, 2023. The Cal-CSIC has submitted a separate BCP to maintain and expand its operation, however, no subsequent changes in law were figured into the request. In order to implement SB 892, additional resources would be needed. The Cal-CSIC has made tremendous progress in reducing the likelihood and severity of cyber incidents that could damage California's economy, its critical infrastructure, or public and private sector computer networks. However, significant work remains. Funding and resources aligned with the level of cyber threat California faces today and tomorrow is critically necessary to best protect our state networks and our critical infrastructure.

An April 2022 Federal Bureau of Investigation (FBI) report stated ransomware actors may be more likely to attack agricultural cooperatives during critical planting and harvest seasons. Since 2021, multiple agricultural cooperatives (grain cooperatives, multi-state grain companies, feed milling and agricultural services) have been impacted by ransomware that halted or slowed production or shut down administrative functions without affecting

production. Initial intrusion vectors were through exploitation of shared network resources or indirectly through compromise of business management software providers.

Cal-CSIC responsibilities—already broad—only become more significant as the cyber threat landscape becomes increasingly active and complex. Among other things, Cal-CSIC is constantly responding to distributed denial-of-service attacks, phishing and spear phishing, Structured Query Language attacks, and cross-site scripting attacks directed not only at California state agencies, but also local governments, and owners of critical infrastructure such as cargo ports and utilities. To support its mission of interagency integration, this proposal includes adding 2 positions for Cal OES. These positions will be dedicated for SB 892 planning and development to directly support food & agriculture sectors as well as water & wastewater sector cybersecurity readiness.

Growth Positions

Branch	Unit | NICE Work Role	Classification	Qty
Mission Support Branch	Professional Services | Cyber Policy & Strategy Planner	Information Technology Specialist III	1
Mission Support Branch	Professional Services | Cyber Policy & Strategy Planner (Grants Analyst)	AGPA	1

E. Outcomes and Accountability

The Cal-CSIC will possess the resources and personnel needed to meet the requirement of SB 892 including: creating a goal for cybersecurity outreach for food & agriculture sectors and water & wastewater sectors; collection, assessment, and analysis of food & agriculture sector and water & wastewater sector cybersecurity challenges and cyber threats; coordinate cybersecurity resources and methods with federal, state, local, and non-profit organizations to protect specifically food & agriculture and water & wastewater sectors; and identify potential funding sources for critical infrastructure cybersecurity defense and analysis. Additionally, the Cal-CSIC will provide the Governor's Office with metrics and success criteria for enhancing cybersecurity defense in the food & agriculture sectors and water & wastewater sectors.

F. Analysis of All Feasible Alternatives

Alternative 1: Approve $531,000 General Fund in 2023-24 and $280,000 in 2024-25 to implement Chapter 820, Statutes of 2022 (SB 892).

Pros:

- Ensure continuation of initial state investment in cyber security and statutory requirements.
- Expands Cal-CSIC's capabilities to analyze need and deliver services to food & agriculture sectors and water & wastewater sectors, while keeping pace with the growing severity and pervasiveness of cyber threats to critical infrastructure.
- In addition to planning services for food & agriculture sectors and water & wastewater sectors, will enable Cal-CSIC to identify cybersecurity gaps and funding sources to support SB 892.
- Reduces the level of cyber risk facing food & agriculture sectors and water & wastewater sectors, which are all part of the attack surface exploited by cyber threat actors in California.

- With expanded cyber threat detection automation and analysis, reduces state remediation costs related to intrusion or cyber breach. As referenced above, average remediation cost per intrusion in 2021 was $1,850,000 (industry reporting on ransomware).

Cons:

- Increase to General Fund.

Alternative 2: Deny this proposal.

Pros:

- No cost to the General Fund.

Cons:

- Cannot meet the requirements of SB 892.
- Increases the cyber risk profile for the state and food & agriculture sectors and water & wastewater sectors.
- Increasing risk that Cal-CSIC will not be able to meet the statutory requirements of SB 892 and/or will have increasingly degraded ability to meet remaining requirements as threat landscape evolves.
- Potential risk of perception among Cal-CSIC partners (especially non-state) that state does not take cybersecurity risk seriously enough to counter threat and keep California safe.

G. Implementation Plan

In July 2023, Cal OES will advertise for positions for this request and provide onboarding training and specialized Cybersecurity Policy and Strategy training.

H. Supplemental Information

No supplemental information.

I. Recommendation

Approve Alternative: 1 for $531,000 General Fund in 2023-24 and $280,000 in 2024-25 to implement Chapter 820, Statutes of 2022 (SB 892).

BCP Fiscal Detail Sheet

BCP Title: Food and Agriculture Sector and Water and Wastewater Sector Cybersecurity (SB 892)

BR Name: 0690-031-BCP-2023-GB

Budget Request Summary

Personal Services

Personal Services	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
Salaries and Wages Earnings - Temporary Help	0	192	96	0	0	0
Salaries and Wages Overtime/Other	0	19	19	0	0	0
Total Salaries and Wages	**$0**	**$211**	**$115**	**$0**	**$0**	**$0**
Total Staff Benefits	0	58	29	0	0	0
Total Personal Services	**$0**	**$269**	**$144**	**$0**	**$0**	**$0**

Operating Expenses and Equipment

Operating Expenses and Equipment	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
5340 - Consulting and Professional Services - External	0	167	84	0	0	0
539X - Other	0	95	52	0	0	0
Total Operating Expenses and Equipment	**$0**	**$262**	**$136**	**$0**	**$0**	**$0**

Total Budget Request

Total Budget Request	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
Total Budget Request	**$0**	**$531**	**$280**	**$0**	**$0**	**$0**

Fund Summary

Fund Source

Fund Source	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
State Operations - 0001 - General Fund	0	531	280	0	0	0
Total State Operations Expenditures	**$0**	**$531**	**$280**	**$0**	**$0**	**$0**
Total All Funds	**$0**	**$531**	**$280**	**$0**	**$0**	**$0**

Program Summary

Program Funding

Program Funding	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
0380 - Emergency Management Services	0	531	280	0	0	0
9900100 - Administration	0	95	52	0	0	0
9900200 - Administration - Distributed	0	-95	-52	0	0	0
Total All Programs	**$0**	**$531**	**$280**	**$0**	**$0**	**$0**

Personal Services Details

Salaries and Wages

Salaries and Wages	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
OT00 - Overtime	0	19	19	0	0	0
TH00 - Temporary Help	0	192	96	0	0	0
Total Salaries and Wages	**$0**	**$211**	**$115**	**$0**	**$0**	**$0**

Staff Benefits

Staff Benefits	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
5150350 - Health Insurance	0	25	12	0	0	0
5150450 - Medicare Taxation	0	3	2	0	0	0
5150500 - OASDI	0	13	7	0	0	0
5150900 - Staff Benefits - Other	0	17	8	0	0	0
Total Staff Benefits	**$0**	**$58**	**$29**	**$0**	**$0**	**$0**

Total Personal Services

Total Personal Services	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
Total Personal Services	**$0**	**$269**	**$144**	**$0**	**$0**	**$0**