STATE OF CALIFORNIA

Budget Change Proposal - Cover Sheet

DF-46 (REV 10/20)

Fiscal Year 2023-24	**Business Unit** 0690, 2720, 7502, 8940	**Department** Office of Emergency Services, California Highway Patrol, Department of Technology, Military Department	**Priority No.**

Budget Request Name 0690-019-BCP-2023-GB 0690-100-BCP-2023-GB 2720-026-BCP-2023-GB 7502-005-BCP-2023-GB 7502-039-BCP-2023-GB 8940-024-BCP-2023-GB	**Program** 0380 - Emergency Management Services, 2050 – Traffic Management, 6230 - Department of Technology, 6911 - National Guard	**Subprogram**

Budget Request Description
California Cybersecurity Integration Center

Budget Request Summary
The Office of Emergency Services, California Military Department, California Department of Technology, and the California Highway Patrol are jointly requesting $28.7 million General Fund ongoing and 17 positions to continue limited-term resources authorized in 2020-21 (including 23 of the 24 previously authorized positions) and enhance resources to support the responsibilities of the California Cybersecurity Integration Center. These resources will allow the Cal-CSIC to lead state efforts to identify and mitigate current and ever-evolving cyber threats, including providing enhanced (1) threat detection, assessment, and research; (2) gap testing and remediation; and (3) incident analysis and response.

Requires Legislation ☐ Yes ☒ No	**Code Section(s) to be Added/Amended/Repealed**	
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 Budget Office	**Date** 8/29/2022	**Reviewed By**	**Date**
Department Director	**Date**	**Agency Secretary**	**Date**

Department of Finance Use Only

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

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

A. Budget Request Summary

The Office of Emergency Services (Cal OES), California Military Department (CMD), California Department of Technology (CDT), and the California Highway Patrol (CHP) are jointly requesting $28.7 million General Fund ongoing and 17 positions to continue limited-term resources authorized in 2020-21 (including 23 of the 24 previously authorized positions) and enhance resources to support the responsibilities of the California Cybersecurity Integration Center (Cal-CSIC). These resources will allow the Cal-CSIC to lead state efforts to identify and mitigate current and ever-evolving cyber threats, including providing enhanced (1) threat detection, assessment, and research; (2) gap testing and remediation; and (3) incident analysis and response.

B. Background/History

Legal Authorities

In 2018, the Cal-CSIC was codified in California Government Code, Chapter 768, Section 8586.5.

By statute, the Cal-CSIC is required to include representatives from Cal OES (including the State Threat Assessment Center (STAC), CDT, CHP, CMD, the Office of the Attorney General (AG), and the California Health and Human Services Agency (CHHS), 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 System (STAS) and the United States (U.S.) Department of Homeland Security (DHS), to establish a cyber-incident response team and safeguard the privacy of individuals' sensitive information. Finally, statute requires the establishment of a Cyber Incident Response Team to serve as California's primary unit to lead cyber threat detection, reporting, and response in coordination with public and private entities across the state.

Mission

The Cal-CSIC's primary mission is 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 our state. The 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. The Cal-CSIC operates in close coordination with the STAS and the DHS - National Cybersecurity and Communications Integration Center, including sharing cyber threat information received from utilities, academic institutions, private companies, and other appropriate sources.

The Cal-CSIC provides warnings of cyberattacks to government agencies and nongovernmental partners, coordinates information sharing among these entities, assesses risk to critical infrastructure and information technology networks, prioritizes cyber threats and supports public and private sector partners in protecting their vulnerable infrastructure and information technology networks, enables cross-sector coordination and sharing of recommended best practices and security measures, and supports cybersecurity assessments, audits, and accountability programs required by state law to protect the information technology networks of California's agencies and departments.

The Cal-CSIC is required to develop a statewide cybersecurity strategy, informed by recommendations from the California Task Force on Cybersecurity and in accordance with state and federal requirements, standards, and best practices. This Task Force, more commonly known as the California Cybersecurity Task Force (CCTF), is designed to represent all sectors and people of the state, as specified above. It is not structured to focus on or exclude any demographic. However, resource constraints force difficult decisions of where to apply those limited resources. The Cal-CSIC has strived to find an efficient balance with the resources it has and has always been eager to respond quickly and effectively to underserved populations such as rural counties. A small number of personnel has meant we are physically concentrated in the Sacramento area, but technology solutions and regional fusion centers have enabled us to significantly broaden this reach.

Initial Cal-CSIC Investment

As a result of the codification of the Cal-CSIC in 2018, Cal OES was able to redirect existing Homeland Security Grant Program (HSGP) and General Fund resources equivalent to eight positions to support the initial steps to get the Cal-CSIC started. This redirection, however, is not sustainable as federal HSGP funding has continued to decline since 2018. Cal OES, CHP, CDT and CMD jointly requested 24 positions and ongoing funding in 2020-21. These positions were authorized, but with only three-year limited-term funding that will expire June 30, 2023. The breakdown of these positions and the 2022-23 funding is as follows:

• Cal OES	12 positions and $8,084,000 General Fund
• CHP	4 positions and $925,000 General Fund
• CMD	8 positions and $1,232,000 General Fund
• CDT	0 positions and $1,268,000 General Fund (the equivalent of six positions)

Accomplishments

1. Staffing: Since receiving funding in July 2020, the Cal-CSIC has been actively hiring subject matter experts in cyber security. Personnel currently on-board include, but are not limited to network engineers, software engineers, cyber threat analysts, forensics experts, application, intelligence experts, and law enforcement professionals.

2. Organizational Structure: The Cal-CSIC has established three distinct functional areas: Cyber Operations Branch, Cyber Threat Intelligence Branch, and a Mission Support Branch.
    a. Cyber Operations Branch (COB)
        i. The COB is the Cal-CSIC's cyber incident response team. The operations team receives and reviews cyber tips and leads from a variety of sources. One primary source of cyber tips comes from California Compliance and Security Incident Reporting System (Cal-CSIRS), the State of California's primary incident reporting system. In 2021 alone, the COB received 2,158 tickets for analysis. Of those, over 420 tickets required various levels of analysis and/or incident response. Two very significant cyber events wherein substantial Cal-CSIC resources were leveraged included SolarWinds and Log4j investigations. Moreover, significant cyber resources were deployed to combat unemployment insurance fraud through the Employment Development Department Pandemic Unemployment Assistance (PUA) fraud investigation.

    b. Cyber Threat Intelligence Branch (CTIB)
        i. The establishment of the CTIB has afforded the Cal-CSIC the opportunity to develop and implement a suite of cyber threat intelligence sharing programs and technological platforms. One critical intelligence sharing program is the

Cal-CSIC's daily production of its "Morning Report". During 2021, the CIB published over 250 morning reports to approximately 1,450 agencies and/or organizations.

ii. In 2021, the CTIB provided monthly tailored threat briefings (classified and unclassified) and authored 48 unique cyber threat intelligence products, on topics ranging from the threat posed by state sponsored cyber actors, the cyber risk from the Internet of Things (IoT) and guidance to mitigate worldwide cyber events such as the vulnerabilities discovered from Solar Winds, Colonial Pipeline, Log4j, and Kaseya attacks involving critical infrastructure and supply chain networks. In addition to the production of its own products, the CTIB also distributes partner products from the Federal Bureau of Investigation (FBI), DHS, Cybersecurity and Infrastructure Security Agency (CISA), Multi State Information Sharing and Analysis Center (MS-ISAC), foreign partner intelligence agencies, and fusion centers from various states across the U.S.

iii. The CTIB also includes a Tactical Intelligence Team regarding cyber threat defense, and in 2021, the Tactical Intelligence Team designed and implemented a near real-time tracking and notification platform to detect cyber vulnerabilities. During its first year of implementation (2021), the Cal-CSIC was able to detect 526 malicious events and notifications PRIOR to an actual breach occurring. This is the primary goal, prevention of a cyber-attack. Of these 526 events, 64 percent were considered "critical" vulnerabilities. Also in 2021, the Tactical Intelligence Team developed and deployed a web-based platform to better automate the acquisition of cyber incidents throughout the state and to better coordinate incident response efforts.

c. Mission Support Branch (MSB)

i. The establishment of the MSB has afforded the Cal-CSIC to become a leader in cyber threat intelligence and cyber incident response operations. MSB is charged with acquisition, configuration, development and maintenance of software and equipment support through defined requirements, architecture design, contract management, procurement, technical support, and training.

3. Technology

The Cal-CSIC has procured the most cutting-edge technological platforms to assist with mission success as set forth in statute. Cal-CSIC tools include but are not limited to contracts with industry leaders in cyber threat detection, intelligence, and mitigation. The Cal-CSIC can perform Dark Web deep threat hunting as well as pursue cyber threat actors across cyber space. These tools have greatly assisted major investigations such as the Employment Development Departments (EDD) Pandemic Unemployment (PUA) fraud. Through the OES' statewide EDD PUA fraud Task Force, billions of dollars have been recovered and returned to the state. The Intelligence and Operations branches worked together along with other state agencies to analyze unemployment insurance fraud and support local, state, and federal criminal investigations. These investigations led to several arrests in 2021, and Cal-CSIC efforts helped identify avenues for anti-fraud measures within California's unemployment insurance program.

a. Through a partnership with Pacific Gas and Electric (PG&E), the Cal-CSIC was able to acquire an Operational Technology (OT) lab which is an exact replica of an electric substation switch (computer system). This OT lab will avail Cal-CSIC, and its partners, the ability to replicate attacks and most importantly defend attacks against our electrical grid.

4. Initiatives
The Cal-CSIC is in various stages of maturity in several program/initiative areas. The programs and/or initiatives listed below are all designed to align with the Cal-CSIC mission, which is to protect the State of California, its economy, critical infrastructure, or public and private sector computer networks.

Cal-Secure. In 2021, the Cal-CSIC, in conjunction with the CDT, 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. In late 2021, Cal-CSIC planned initial steps to begin a closer, more formalized, and more collaborative working relationship with CDT's Office of Information Security to jointly implement Cal-Secure and align our efforts with Cal-Secure priorities and track our progress toward Cal-Secure success measures. Cal-CSIC led a bi-weekly working group for this purpose in early 2022 and has already collaborated and coordinated with CDT OIS on multiple joint initiatives through this forum.

Cyberspace Operational Protected Systems (COPS). Resulting from "Blue Leaks", a massive data breach involving hundreds of law enforcement (LE) agencies, the Cal-CSIC developed and leveraged its technological tools, to scan and secure the external networks of hundreds of our LE partners. As a result, these LE agencies and their networks are better protected against a cyber-attack.

State Election Risk and Vulnerability Evaluation (SERVE). In conjunction with the OES led Election Security Task Force, the Cal-CSIC established SERVE. The Cal-CSIC performed attack surface vulnerability assessments for all 58 counties and their election computer systems. Nine counties responded requesting service. Relying upon open source, United States Intelligence Community (USIC) and private sector cyber threat intelligence, the Cal-CSIC was able to reduce the risk of state sponsored or criminal cyber actor disrupting our electoral process.

Industrial Control Systems Analytics Program (ISAP). A program designed to protect the Operational Technology (OT) environments of our states most critical of critical infrastructure.

Rapid Attack Vulnerability Enumeration (RAVEn). A program designed to examine cyber risk and illuminate vulnerabilities which serve as potential targets to be exploited from cyber threat actors.

Cybersecurity Maturity Assessment Program (CMAP). This program is designed to provide a cyber-security analysis or "scorecard" to assist with the level of cyber risk for that entity. This scorecard can then be used by executive leadership to guide their cyber investment justifications with the goal of cyber risk reduction.

Cybersecurity Capability Maturity Model (C2M2). Working in conjunction with the Pacific Northwest National Laboratory (PNNL) and the U.S. Department of Energy (DOE), the Cal-CSIC is developing C2M2 which is designed to *evaluate, prioritize, and improve* cybersecurity maturity across CA's critical infrastructure sectors and partners. C2M2 was established to improve electricity subsector cybersecurity capabilities and to better understand the cybersecurity posture of the grid thus reducing the cyber risk posed by state sponsored and criminal actors.

From this program, we can better forecast strengths and weaknesses of the entity and facilitate recommendations and areas of improvement needed to meet stronger security level requirements.

This provides us a more complete picture of the cyber threat landscape of CA as we can see maturity levels across all of California. Further analysis of this combined with findings from RAVEn and threat intel-sharing can identify common weak links or common strong points with hard data and metrics to support findings. This leads to further enablement of strong intelligence sharing and recommendations to sector or geographical levels that can improve security posture on a much larger scale.

Emergency Support Function – 18 (ESF 18). To ensure state resiliency from cyber-attack, the Cal-CSIC developed and completed ESF-18. ESF-18 establishes a unified command structure and framework to coordinate the states response to a significant cyber related event.

Validation & Analysis of Lifeline Infrastructure- Data Sharing Initiative-State of California (VALIDS). As part of an automated information sharing initiative, VALIDS includes integration with ESF-18 reporting at the Cal OES headquarters level, accomplished through posting California specific incident tracking statistics. Cal OES and the STAC continue to be in close coordination on the completion of this project no later than the third quarter of FY 2022-23.

The California Cybersecurity Task Force. The California Cybersecurity Task Force is a cybersecurity advisory body for California composed of subcommittees focused on goals and objectives aligned to state (and federal) cybersecurity objectives and planning. This state Cybersecurity Task Force is intended to be comprised of subject matter experts and executive representatives from Federal, State, local, and tribal government, private industry, academia, and law enforcement in California. Fully supporting and sustaining the Cybersecurity Task Force requires substantial time and effort from Cal-CSIC personnel but brings large dividends back to the state in the deep and broad expertise of its members.

Analysis of Problem

Resource History

(Dollars in thousands)

Program Budget	PY – 4	PY – 3	PY – 2	PY-1	PY	CY
Authorized Expenditures				11,061	11,508	11,508
Actual Expenditures				11,061	11,508	11,508
Revenues				0	0	0
Authorized Positions				24	24	24
Filled Positions				24	24	23
Vacancies						1

C. State Level Consideration

Cal OES' mission is 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. As documented above, 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 we face today, and tomorrow is critically necessary to best protect our state networks and our critical infrastructure.

This proposal will enable the Cal-CSIC to broaden its reach into underserved communities through both technological solutions, opportunities to diverse groups through the CCTF, and organized events to influence state cybersecurity policy and practices.

In comparison to other states, California ranks toward the bottom for cybersecurity resources in proportion to our population. In a recent data call through the National Governors' Association, most respondents indicate actual or necessary growth in their cyber centers.

State/Organization	Personnel	Region Population (2022)	Per Capita Rate (per million)
New York City Cyber Command	250	8,865,000	28.20
Wisconsin	115	5,935,064	19.38
Alaska	12	731,011	16.42
South Dakota	12	901,165	13.32
New Jersey	54	9,200,000	5.87
North Carolina	40	10,678,831	3.75
Arizona	20	7,303,398	2.74
New York State Joint Security Operations Center (JSOC)	27	20,115,000	1.34
California	38	39,950,000	0.95
Virginia	4	8,750,000	0.46
Washington	2	7,901,429	0.25

Since its inception, the Cal-CSIC has grown through essentially three developmental stages:

1. Initial formation funded by a mixture of Homeland Security Grant Funding and state General Fund prior to the initial investment in 2020-21. This initial stage enabled us to build a framework for a new organization, hire a core cadre of start-up staff, and begin basic elements of our mission.

2. The second stage is the current three-year limited-term investment in which the Cal-CSIC made substantial progress, from a staffing, technological and initiatives perspective. During this period, the Cal-CSIC began executing many elements of its mission and formed plans for continued growth to both meet original statutory requirements and address emerging threats and challenges. As we have learned through our accomplishments, our challenges, and through relationships established at various levels of government, the Cal-CSIC has a far greater understanding of the threat environment, and the unique and complex cybersecurity needs of California. As a result of our three years of work, coupled with industry leader forecasts, we recognized utilization of existing resources would only sufficiently address some, but not all, of the Cal CSIC's statutory requirements at an appropriate level to reduce risk. Simply put, the vastness of the State of California and its relative cyber risk demands a commensurate number of cyber professionals and tools which are aligned with mission requirements of the Cal-CSIC. Current staffing levels were sufficient to "start-up" this endeavor, however; ongoing resources are necessary to continue to identify and mitigate current and future cyber threats and ensure all statutory requirements are met more efficiently and effectively.

3. The third phase represents the state's ongoing commitment to cyber security. This plan contemplates existing and future requirements and lessons learned since the inception of the Cal-CSIC. It also reflects a changing and continual increasing threat landscape, where cybersecurity plays an even bigger role than many envisioned four years ago. As outlined below, many previously theoretical threats are manifesting in the real world and impacting California daily. Lastly, as Cal-CSIC customers interact with us and their understanding of our capabilities and value grow, their interest in and demand for our services also grows in a way that is not completely tied to the threat landscape. This proposal will grow the Cal-CSIC from the current 24 positions and $11.5 million to 40 positions and $28.7 million, as outlined below:

    - Cal OES 26 positions (12 existing and 14 new) and $23,213,000 General Fund
    - CHP 3 positions (a reduction of one) and $849,000 General Fund
    - CMD 8 positions (all existing) and $1,318,000 General Fund
    - CDT 3 positions (all new) and $3,360,000 General Fund

Current Cyber Threat Environment

1.) <u>National Cyber Threat Overview</u>
Cyber threats to California's security are increasing in frequency, scale, sophistication, and severity. The cyber threat landscape is vast and deep and regularly influenced by the world around us. When the COVID-19 pandemic began, an uptick was observed in targeting of healthcare and research and development. Now, the situation unfolding in the Ukraine shows how tightly the geopolitical and cyber world are intertwined[1].

The ranges of cyber threat actors, methods of attack, targeted systems and victims are also expanding. According to the U.S. government National Cyber Strategy, cyber threats will continue to increase in the coming years, as more devices are connected to the internet and threat actors grow their attack capabilities. Attack methods such as

[1] Mandiant - Three Year Cybersecurity Trending for California (2020-2022), pg 12

ransomware and malware have spread globally resulting in major disruptions and exfiltration of sensitive data.

Attacker tactics, techniques, and procedures (TTPs) in California's cyberspace have not changed dramatically over the past three years, but the overall trends are still evolving. For example, adversary organizations are migrating to the cloud at an increasing rate. Notable observations from Mandiant are listed below[2]:

2020

- Malware authors are innovating—possibly to evade detection technologies—and not just relying on updates to existing malware.
- Cyber criminals that historically targeted personal and credit card information are increasingly turning to ransomware as a secondary source of income. Cyber criminals are also outsourcing tasks to monetize operations faster.
- To expand the way they monetize operations, attackers have been observed targeting corporate reward systems to steal gift cards. These gift cards are then resold or used to make direct purchases.

2021

- As ransomware operators were attacking state and municipal networks alongside hospitals and schools, a global pandemic response to COVID-19 necessitated a move to remote work for a significant portion of the economy.
- Ransomware has evolved into multifaceted extortion where actors not only deploy ransomware encryptors across victim environments, but also employ a variety of other extortion tactics to coerce victims into complying with demands.
- Threat actors took advantage of infrastructure supporting work-at-home with an increased focus on vulnerability exploitation.

2022

- Critical vulnerabilities such as "Log4Shell" highlight the dangers of the unknown and the complexity of patching. Log4Shell is a vulnerability in the Log4j component of Apache, a popular webserver platform. Log4Shell has been heavily exploited since December 2021. This has resulted in major cyberattacks and disruptions worldwide and in California. Cal-CSIC has assisted state agencies running webservers affected by the vulnerability. The supply chain is as attractive as ever target, providing a potential entry point into multiple vendors.
- Ransomware and multifaceted extortion continue to be concerning. There was an observable increase in targeting of virtualization infrastructure and offer mitigations. Guidance on ransomware preparedness (via red teaming) and recovery operations was published to address this issue.

The following statistics provide a brief snapshot of the cybersecurity threat we face today:

- The average cost of a data breach rose from $3,860,000 in 2020 to $4,240,000 in 2021.

[2] Mandiant - Three Year Cybersecurity Trending for California (2020-2022), pg 3

Analysis of Problem

- Ransomware attacks increased by an estimated 127 percent in 2021.
- The remediation costs per incident associated with a ransomware attack increased from $761,106 in 2020 to $1,850,000 in 2021.
- Social engineering attacks posed the greatest threat to public administration, accounting for 69 percent of the data breaches experienced in the public administration sector during 2021.
- A new ransomware attack is estimated to have occurred somewhere globally, every 11 seconds during 2021.
- Double extortion attacks accounted for 8.7 percent of all reported ransomware incidents globally, in 2020 but increased 81 percent by the second quarter of 2021.

2.) Significant National Cyber Incidents
The below list of key incidents and issues created some of the most significant impacts to the U.S. economy in 2021:

- July 2021, hackers exploited a vulnerability in Kaseya's virtual systems/server administrator (VSA) software allowing them to conduct a ransomware attack that infected approximately 1,500 small and midsized businesses globally with REvil ransomware.
- May 2021, major multinational meat processing company JBS SA became the victim of a REvil ransomware attack that resulted in all of their U.S.-based meatpacking plants to shut down until June 2021.
- May 2021, Colonial Pipeline became the victim of a DarkSide ransomware attack that resulted in the pipeline being shut down for five days.
- February 2021, unknown hackers attempted to raise levels of sodium hydroxide in the water supply of Oldsmar, Florida after gaining unauthorized access to the network by exploiting a remote system access.

3.) Significant California Cyber Incidents

a. 2021. The Cal-CSIC received 2,158 event leads from CAL-CSIRS, the state's security incident reporting system, of which 430 were identified by Cal-CSIC as cyber incidents requiring various levels of Cal-CSIC incident response or analysis. An additional 30 cyber incident notifications were received from a variety of sources. These 460 incidents represented an approximate increase of 265 percent from 2020 when we saw 126 incidents. Each of these 460 incidents required Cal-CSIC incident response actions including: 15 post-incident consults, 5 incident response events, 6 Mission Resource Taskings (MRT), and 4 assessments. Post-incident consults involve a minimum of 24 personnel hours per incident, but some can be much more involved and can require up to 80 hours. Incident response events which do not require MRTs require 2-3 Cal-CSIC personnel for up to three days, with 80 hours maximum for analysis and report writing. MRTs are large enough that they exceed Cal-CSIC's capacity to respond and require additional resources from CMD (typically 2-3 additional personnel), but still require 2-3 Cal-CSIC personnel for up to three days, with 80 hours maximum for analysis and report writing. Assessments are generally a response to a request for assistance that does not necessarily involve an intrusion or breach, but still require 2 personnel doing a combined 16 hours of work.

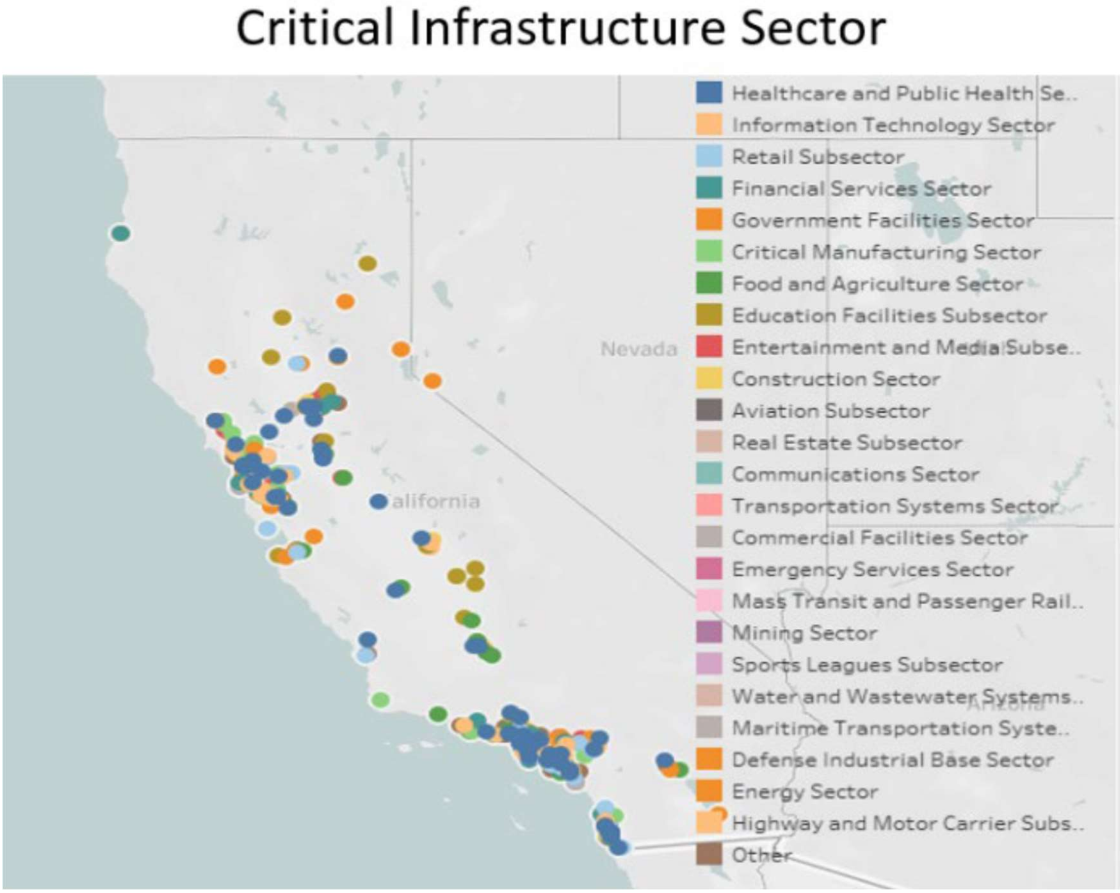
b. Within these 460 incidents in 2021, the most prevalent type of cyber-attack observed was ransomware, which accounted for 43 percent or 198 incidents. We lack enough detailed and thorough data going before 2021 to make a comparison, but globally ransomware increased 127 percent from 2020 to 2021 so we can safely assume that rate was similar for California. Rounding out the top three incident types in 2021 were corporate and personal data breaches at 28 percent and phishing/vishing/smishing incidents at 13 percent.

Additionally, the Healthcare and Public Health sector was the most targeted sector accounting for 16 percent or 67 observed incidents, followed by the Information Technology sector with 10 percent or 42 incidents, and lastly the Financial Services sector with 9 percent or 38 cyber incidents.

Regarding the cyber threat to the Healthcare Sector, two significant events occurred in California in 2021.

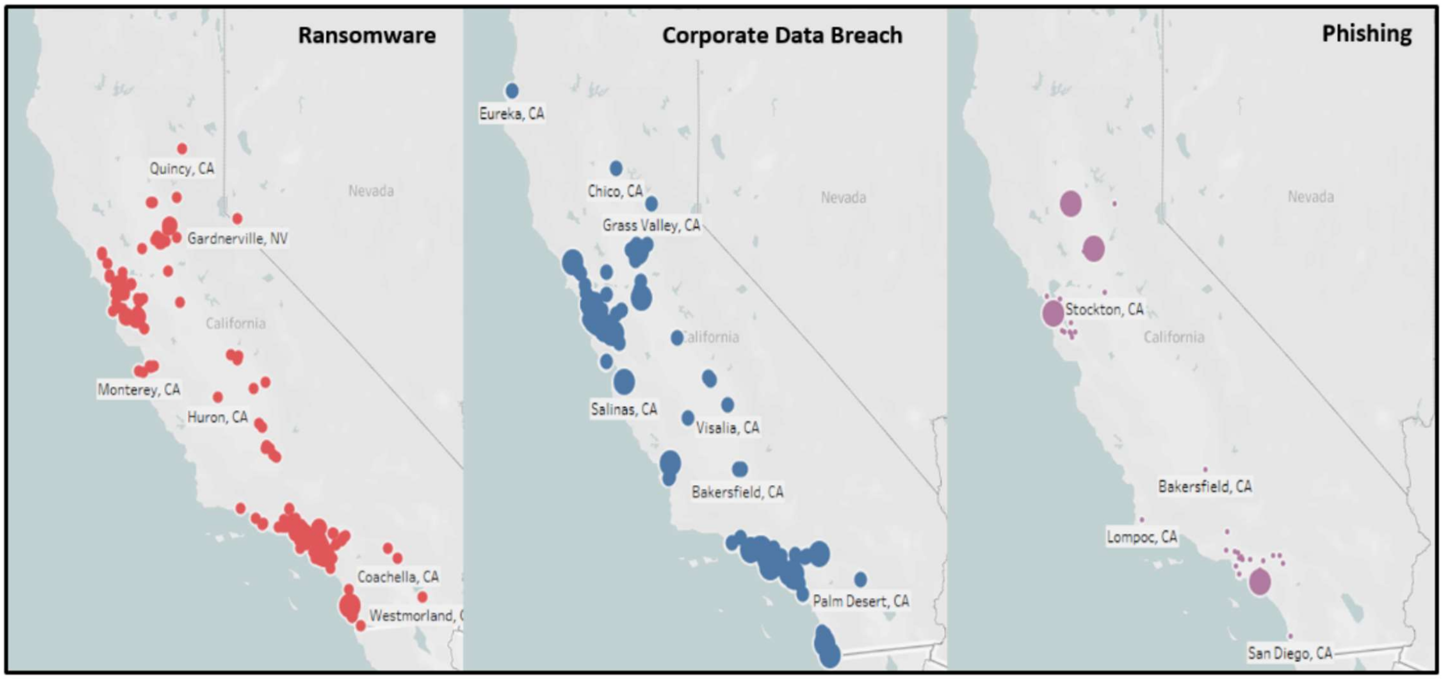
- May 2021, Scripps Health, a nonprofit healthcare provider headquartered in San Diego, suffered a significant cyber-attack. Scripps Health system consists of five hospitals, 19 outpatient facilities, and provides healthcare services to over half-million patients and over 2,600 affiliated physicians.
- October 2021, the Los Angeles branch of Planned Parenthood (PPLA) disclosed their networks were breached by a ransomware attack. Initial investigation revealed at least 400,000 patient records were stolen.

The chart below illustrates the regions of California that experienced cyber incidents during 2021. The highest concentration of cyber incidents was observed in the Los Angeles and the San Francisco/Bay Area regions of California; almost certainly due to the high number of corporate presence and population density.


Critical Infrastructure Sector
Nevada
alifornia
Healthcare and Public Health Se..
Information Technology Sector
Retail Subsector
Financial Services Sector
Government Facilities Sector
Critical Manufacturing Sector
Food and Agriculture Sector
Education Facilities Subsector
Entertainment and Media Subse..
Construction Sector
Aviation Subsector
Real Estate Subsector
Communications Sector
Transportation Systems Sector
Commercial Facilities Sector
Emergency Services Sector
Mass Transit and Passenger Rail..
Mining Sector
Sports Leagues Subsector
Water and Wastewater Systems..
Maritime Transportation Syste..
Defense Industrial Base Sector
Energy Sector
Highway and Motor Carrier Subs..
Other

Analysis of Problem

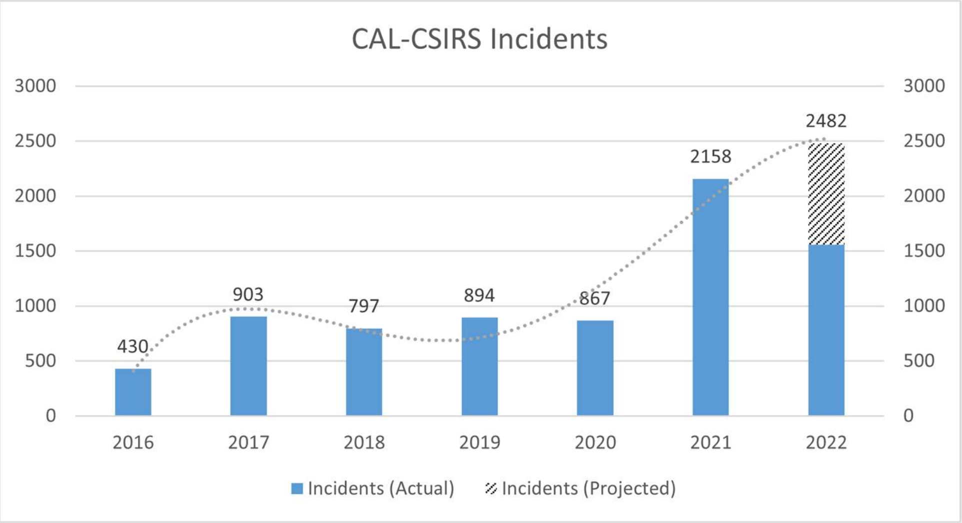
The chart below illustrates the top three cyber incident types observed in California during 2021 and the region in which they were observed.



c. 2022. During the first half of 2022, the Cal-CSIC received 1,557 cyber event leads from Cal-CSIRS, plus an additional reported 223 cyber incidents received from other sources. Of those 223 cyber incidents listed above, 133 were considered cybercrimes and 90 as data breaches. In summary, ransomware was by far the most frequent cybercrime, accounting for 56 percent of all cyber incidents in California in the first half of 2022. Information Technology, Professional/Non-Professional Services, Commercial Facilities, and Government Facilities Sectors were the most frequently targeted for attacks. Investment crimes in California climbed sharply in the first half of 2022 in both victim loss and number of reported crimes from the first half of 2021. Lastly, tech Support crimes have also risen in the year-over-year period, with reported victim losses nearly doubling for Californians. At this rate of rise, it is projected nearly 2,500 CSIRs leads will be received.

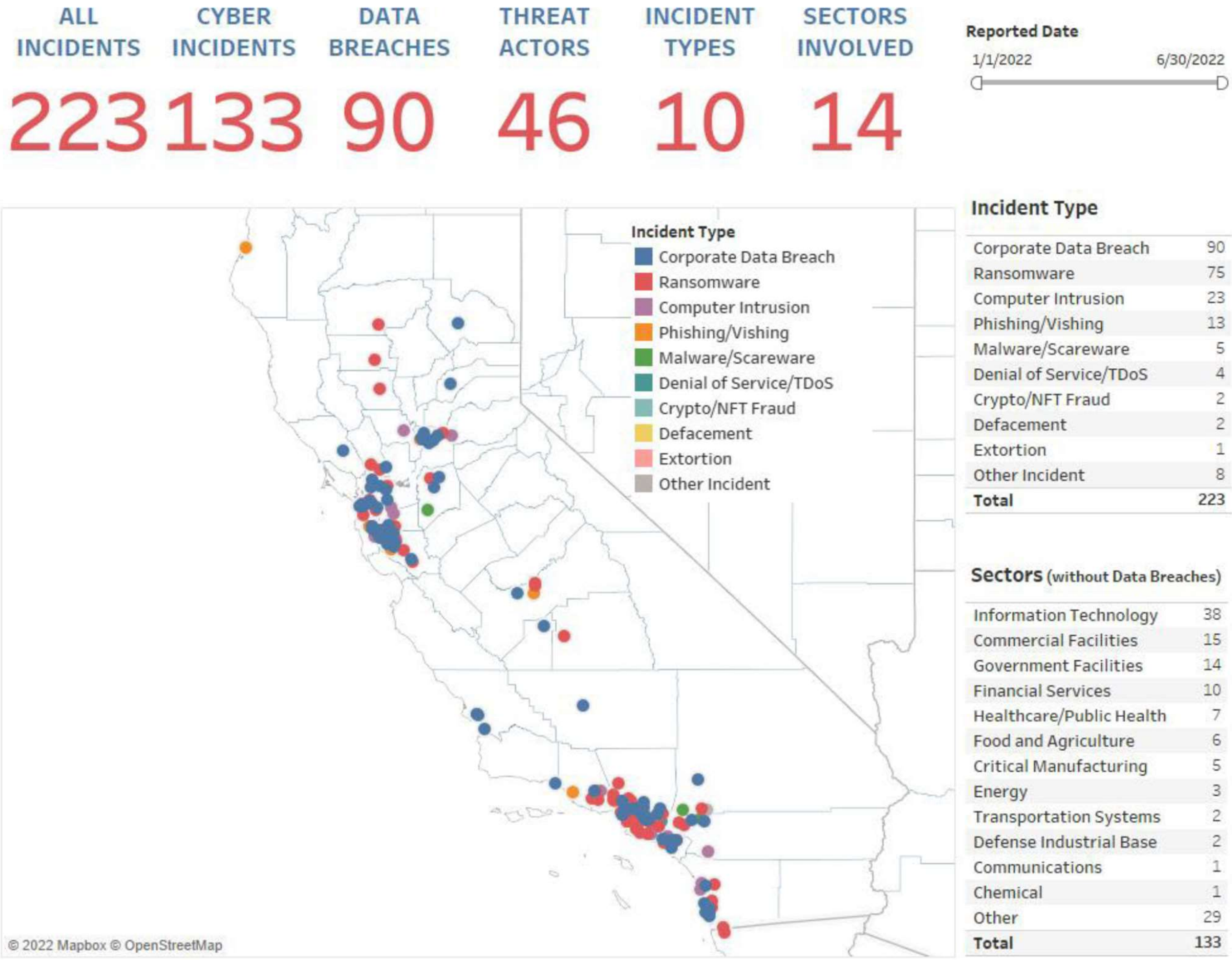
The chart below provides historical context of Cal-CSIRS cyber reporting, since 2016. The total number for 2022 is a projection based on a total of 1557 incidents recorded through August 17, 2022 (approximate average rate of 6.8 per day).

Analysis of Problem



Based on the current rate of growth, we estimate incidents will increase by approximately five percent in 2023 and another 12 percent beyond that in 2024.

The chart below shows the first half of 2022 cyber incident data by geographical location, incident type, and critical infrastructure sector for the 223 cyber incidents mentioned above.



ALL INCIDENTS	CYBER INCIDENTS	DATA BREACHES	THREAT ACTORS	INCIDENT TYPES	SECTORS INVOLVED
223	133	90	46	10	14

Reported Date
1/1/2022 6/30/2022

Incident Type	
Corporate Data Breach	90
Ransomware	75
Computer Intrusion	23
Phishing/Vishing	13
Malware/Scareware	5
Denial of Service/TDoS	4
Crypto/NFT Fraud	2
Defacement	2
Extortion	1
Other Incident	8
Total	223

Sectors (without Data Breaches)	
Information Technology	38
Commercial Facilities	15
Government Facilities	14
Financial Services	10
Healthcare/Public Health	7
Food and Agriculture	6
Critical Manufacturing	5
Energy	3
Transportation Systems	2
Defense Industrial Base	2
Communications	1
Chemical	1
Other	29
Total	133

In summary, no industry sector was spared from ransomware attacks. Sectors such as healthcare, educational facilities, information technology, government and military contractors were all targeted. The Professional and Non-Professional sub-sectors along with Construction ("Other" sector) were hit particularly hard by ransomware, accounting for 25 attacks (33 percent of ransomware attacks) in the first half of 2022. Attacks against the Information Technology (29 percent). Other (22 percent), Government Facilities (including Educational Facilities, 11 percent), and Commercial Facilities (including Retail, 11 percent) sectors accounted for nearly three-quarters of all cybercrimes.

Two other sectors of critical importance to the economic prosperity of California—Food and Agriculture and Healthcare and Public Health—each accounted for five percent of all incidents in the first half of 2022.

Protection of Critical Infrastructure

An area of prioritization for the Cal-CSIC is ensuring the lights stay on, the water keeps flowing and essential services of our daily lives remain resilient and without disruption caused by either a natural disaster or manmade (cyber, terrorism) event.

In conjunction with DHS' National Critical Infrastructure Prioritization Program (NCIPP) and the STAC's Critical Infrastructure Program (CIP), we have identified and qualified all the critical infrastructure assets in the state. As such, 1,309 assets have been identified and categorized. Of these, 548 are lifeline sectors, such as communications, energy, transportation, water and wastewater systems. They are further broken down:

- Communications – 42 assets
- Energy – 174 assets
- Transportation – 136 assets
- Water and Wastewater Systems – 196 systems

As we have seen in recent years, cyber-attacks on critical infrastructure can have devastating impacts on many sectors of our economy. A recent example from the energy sector is the cyber-attack on the Colonial Pipeline. In May 2021 a ransomware attack against a U.S. fuel pipeline operator, Colonial Pipeline was reported. This attack affectively shut down a major oil pipeline, referred to as the "jugular of the U.S. pipeline," that supplies nearly half of all the gasoline, diesel, jet fuel and other refined products from the Gulf Coast to the eastern and southern U.S. The shutdown of this pipeline temporarily halted the delivery of critical fuels to potentially 38 to 52 percent of the entire U.S. population.

An example from the Water and Wastewater Systems is the February 2021 cyber-attack, wherein unknown hackers attempted to raise levels of sodium hydroxide in the water supply of Oldsmar, Florida after gaining unauthorized access to the network by exploiting a remote system access.

As referenced above under initiatives, the Cal-CSIC identified a cybersecurity gap regarding critical infrastructure and has developed two specific programs (CMAP and C2M2) to assist in closing that gap.

Analysis of Problem

Cyber Threat Outlook

As we attempt to forecast the cyber threat to the State of California, we are starkly reminded that there are many threat actors we face, with a wide variety of motivations, tools, and tactics.

Nation-State actors will deploy necessary cyber resources to advance their national security, political and economic agendas. The following is snapshot of the top four Nation-State actors and the advanced persistent threat they pose to California[3]:

Russia: Russia will maintain an aggressive posture throughout the remainder of 2021 and into 2022, with a sustained emphasis on targeting North Atlantic Treaty Organization (NATO), Eastern Europe, Ukraine, Afghanistan, and the energy sector. The U.S. government attributed the UNC2452 attack (also referenced as the SolarWinds supply chain compromise incident) to Russia, which demonstrates Russia can achieve widespread impact. We expect supply chain and software supply chain environments to continue to be targeted by Russia next year. Additionally, UNC2452's manipulation of authentication methods in hybrid cloud/on-premises environments highlight innovative tactics, leading us to believe the level of sophistication and scope of Russian operations will expand.

Iran: Iran will use its cyber tools in a much more aggressive manner to promote regional interests. Information operations attributed by the U.S. to Iran in 2020 and 2021 demonstrated more aggressive tactics than previously seen. Iran will also continue to target Israel and others in the Middle East. They've shown their capability and willingness to use destructive malware, so we expect them to take advantage of any opportunities that are presented. Ultimately, we'll see Iran trying to create more of a power balance shifted to its own interests. We have seen them targeting abroad, but their targeting will most likely be regional throughout 2022.

China: China will continue to be very aggressive, supporting the Belt and Road Initiative using cyber espionage. Now that the Ministry of State Security (MSS) and the People's Liberation Army (PLA) have completed most of their reorganization, their operations are going to become much more focused. China has shown a willingness to scale their operations and take steps that they were previously unwilling to take. As geopolitical tensions continue to rise, the big question is "When are we going to see China flex some of their known but as-yet-unused destructive capabilities?"

North Korea: North Korea, with its geographical, international, and financial challenges, is willing to take a lot of risks. In 2022, we expect to see North Korea flex its cyber capabilities to make up for its lack of other instruments of national power. The North Korean cyber apparatus will continue to support the Kim regime by funding nuclear ambitions and gleaning strategic intelligence.

Criminal threat actors, mostly motivated by money, will remain one of the top threats we face in California. Ransomware is going to continue to evolve and increase in severity. Ransomware threat has grown significantly throughout the past decade, and it will continue its upward trend4. Ransomware actors are becoming increasingly aggressive, turning these once relatively simple attacks into more elaborate, lucrative, and multifaceted extortion operations. U.S. and international efforts are underway, but these mitigation efforts are having little to no effect to the relatively new "ransomware-as-service" model5.

[3] Mandiant. 14 Cyber Security Predications For 2022 and Beyond, pg. 4

[4] Mandiant. 14 Cybersecurity Predictions for 2022 and Beyond. Pg 2

[5] Mandiant. 14 Cybersecurity Predictions for 2022 and Beyond. Pg 8

Analysis of Problem

It is forecasted that cyber-attacks against operational technology (OT) networks will increase mostly. In 2021, Mandiant observations reveal that low sophistication threat actors learned they could create big impacts in the OT space, even bigger than their intended consequences. As such, it is expected threat actors will explore the OT space in 2022 and beyond and increasingly deploy ransomware against those networks. Attacks against OT systems are largely attacks against critical infrastructure networks. Attacks against OT environments can cause serious disruption and even threaten human lives, increasing the pressure of organizations to pay a ransomware.

Cyber espionage, often referred to misinformation/disinformation, will remain a consistent threat in California. These campaigns are largely influenced by world events and designed to influence Californians on a wide variety of topics. As deep-fake technologies become more widely available, criminal and espionage actors will increasingly integrate manipulated media into their operations to make social engineering more convincing, which will most likely defeat some automated identity verification systems.6

In the coming years, we expect to see a continued growth of Internet of Things (IoT) devices, many of which will be inexpensive and created without cybersecurity in mind. Because all of these devices are connected, we will see the general attack surface expand greatly with the potential for serious impact7. We have observed several case examples wherein thousands of IoT devices were leveraged to create a Distributed Denial of Service (DDOS) attack against an intended target.

If we use the workload of the CTIB team as an indicator, demand for services has been significantly increasing while the team, as effective as they are, is potentially seeing a plateau of their capacity. We interpret this as a resource being maximized facing increasing demand rather than any change in performance. In fact, the breadth and types of intel support has continued to become more sophisticated, and event support has increased. Increasing subscriber demand can be interpreted as an indicator of general awareness of the threat landscape, but also as an indication of the critical necessity of the CTIB team's work.

Year	Cyber Threat Intelligence Service Subscribers[A]			Cyber Threat Intelligence Production					Major Joint Events Supported (Exercises, National Security Events)
	Morning Report Subscribers	Monthly Threat Brief Subscribers	Intelligence Product Distro List	Advisories	Executive Summaries	Cybersecurity Bulletins	Alerts[B]	Notifications[C]	
2019	No data	No data	No data	7	1	2	No data	No data	
2020	487	470	873	7	3	1	2	No data	2
2021	854	880	1,317	9	5	2	49	374	7
2022[D]	1269	1,290	1,806	1	5	9	17	209	5
2022[E]	*2032*	*2065*	*2891*	*2*	*8*	*14*	*27*	*335*	*8*

A. Subscriber data not available prior to 2020
B. Alerts metric not tracked until 2020
C. Notification's metric not tracked until 2021
D. Data as of 17 Aug 2022
E. Data projected for 2022 based on average monthly rate

[6] Mandiant. 14 Cybersecurity Predictions for 2022 and Beyond. Pg 5

[7] Mandiant. 14 Cybersecurity Predictions for 2022 and Beyond. Pg 7

Analysis of Problem

Gaps

During each phase of Cal-CSIC's growth to-date we have encountered, analyzed, and planned how to close capability gaps. We define these gaps as differences between how we interpret our statutory mandate versus our actual capability and mission effectiveness. As mentioned before, we see this through the lens of three distinct phases:

Phase 1) launch and initial growth prior to 2020-21 investment,
Phase 2) 2020-21 to 2022-23 investment funded by General Funds and HSGP, and
Phase 3) 2023-24 and on-going investment.

While many gaps have been closed in the first two phases, many remain, and we anticipate a significant shortfall in capability.

The Cal-CSIC staffs less than one (0.95) cybersecurity personnel per million in population. This is extremely low compared to states like Wisconsin, Alaska, and South Dakota with staffing rates above 10 per million. Additionally, the New York City Cyber Command is staffed at 28.20 cybersecurity personnel per million people in the city, on top of the New York State Joint Security Operations Center (JSOC) with 1.34 cybersecurity personnel per million people in the state.

California is massive in physical size, population, and economy. Its size along with a myriad of unique assets including: 11 seaports; 1 U.S border; agriculture industry, technology industry, and a complex critical infrastructure create a higher-than-average demand on cybersecurity while staffing numbers lag far behind the norm.

As indicated above, incidents including those requiring Cal-CSIC response continue to increase at a rate that nearly doubles over six years. Cal-CSIC intelligence services continue to see increasing demand at a rate that is on pace to be five times what it was in 2020. This is due to three primary factors:

Factor 1) an evolving threat landscape which could not be fully predicted three years ago,
Factor 2) increasing customer demand as they become aware of and appreciate our services, and
Factor 3) our increasingly sophisticated understanding of our mission and resources necessary to execute it successfully.

It should be noted that the Cal-CSIC is still a relatively new organization and function within the state, and our collective understanding of how it can and should work has evolved tremendously since our inception. Despite these growing demands, our personnel and resources will not grow to keep pace without additional investment. Listed below are areas where we still see capability gaps.

1. Build and maintain an asset model for the state, aka "California cyber terrain":
    a. Gap: the Cal-CSIC has a partial picture of California's cyber terrain
    b. Impact:
        i. will miss emerging threats and early stages of major incidents
        ii. will be dependent on voluntary reporting from outside parties and
        iii. will be in a reactive posture unable to prevent attacks from occurring in some cases
2. Establish Semi-Automated Processes:
    a. Gap: as the Cal-CSIC program matures, the demand for automation shifts from internal to external with customers and partners. Demand will become unmanageable
    b. Impact: the lack of available automation will result in precious resources being wasted using ad-hoc, manual, one-off approaches

3. Maintained state-level cyber security scorecard:
    a. Gap: assessment capabilities and stakeholder partnerships lack maturity
    b. Impact: without a thorough statewide baseline of cyber risk, priority-based resource allocation suffers
4. Incident Response Capacity Scaled to Typical Demand, Surge, and Projected Threat:
    a. Gap: Increasing incident workload is outpacing current staffing levels.
    b. Impact: the Cal-CSIC's ability to provide critical response services diminishes over time.
5. Intelligence Analysis Capacity Scaled to Typical Demand, Surge, and Projected Threat:
    a. Gap: The CTIB team saw demand for their products grow by 51% from 2020 to 2021 and we project demand to grow to 186% of the current level by 2024. Again, workload is outpacing current staffing levels.
    b. Impact: leaders will be less informed when making critical cybersecurity risk decisions.
6. Full multi-sector coverage:
    a. Gap: Without an increase of resources, our ability to best protect our critical infrastructure as categorized previously in the "Protection of Critical Infrastructure" section will be significantly impacted.
    b. Impact: cybersecurity risks to certain sectors like water infrastructure will not be tracked at adequate levels
7. Fully leverage Cybersecurity Task Force:
    a. Gap: The Cybersecurity Task Force will be underutilized due to staffing constraints and prioritization of staffing resources.
    b. Impact: partner commit levels will decrease causing reputational damage to Cal-CSIC, OES, and the state.
8. Full application of Operational Technology (OT) and Forensics Labs:
    a. Gap: the resources required to processing OT and Forensics Lab workloads will be outpaced by projected demand
    b. Impact: These critical resources will become underutilized
9. OT lab fully representative of all sectors:
    a. Gap: The OT lab is in its initial implementation phase
    b. Impact: not all sectors are fully represented.
10. Robust Cal-CSIC-hosted cybersecurity exercise program:
    a. Gap: the demand (invitations to participate/requests to host) towards cybersecurity exercises and joint operations is outpacing current staffing levels
    b. Impact: these vital programs that benefit the state and the nation will become less effective.

Summary

The vastness of the State of California, coupled with its global economic impact, is a prime target for state-sponsored and criminal actors. The proposal set forth strikes the appropriate balance of maintaining what we have begun, while increasing the necessary resources (staff and technology) commensurate to the level of cyber risk we face. Current staffing levels were sufficient to "start-up" this endeavor, however; additional resources are requested to identify and mitigate current and further cyber threats more efficiently and effectively.

E. Outcomes and Accountability

By securing the additional 17 positions, the Cal-CSIC will be positioned to comply with statutory requirements and have sufficient resources to respond to the ever-increasing cyber threat. This will allow for the establishment of a well-trained team, housed at the Cal-CSIC Mather, CA location that will draw on competencies and resources from numerous technical backgrounds, assist in analyzing cyber threat intelligence, and prepare, respond, and mitigate cyber threats to California's cyber infrastructure.

With additional resources and improved ability to capture and analyze data, the Cal-CSIC will develop quantitative and qualitative metrics to measure the economic impact and overall cyber risk for relevant regions and populations to ensure cyber resources are deployed to high-risk areas and institutions. The Cybersecurity Task Force will be a key mechanism for identifying unserved or underserved regions and populations. The additional positions will assist in fully leveraging the refurbished and improved main office workspace and newly formed forensics lab, expand the specialized individual skills of Cal-CSIC incident responders, provide additional support in cyber threat intelligence gathering and sharing threat intelligence with Cal-CSIC partners and customers, and assist in identifying cyber risks based on evolving and emerging cyber threats. Additionally, the extra positions will assist in conducting forensic analysis on infected/compromised physical and virtual hardware to determine the extent and impact it caused and assist with mitigating controls to properly contain cyber threats against California's critical infrastructure and economy.

F. Analysis of All Feasible Alternatives

Alternative 1: Approve $28.7 million General Fund ongoing and 17 positions to continue limited-term resources authorized in 2020-21 (including 23 of the 24 previously authorized positions) and enhance resources to support the responsibilities of the Cal-CSIC. These resources will allow the Cal-CSIC to lead state efforts to identify and mitigate current and ever-evolving cyber threats, including providing enhanced (1) threat detection, assessment, and research; (2) gap testing and remediation; and (3) incident analysis and response.

Pros:

- Ensure continuation of initial state investment in cyber security and statutory requirements .
- Expands California's capabilities to analyze need and deliver services across the state, keeping pace with the growing severity and pervasiveness of cyber threats more equitably .
- Shift from a more reactive posture to a more proactive posture in anticipating and stopping cyberattacks before they result in harm .
- In addition to adding depth, will enable Cal-CSIC to add breadth of services adding capabilities that it did not previously wield making a more complete suite of services.
- Reduces the level of cyber risk facing the state, its 225,000 employees, multiple large networks (including CGEN, CALNET, and CENIC), more than 80 state-provided network services, and over 1 million endpoints, which are all part of the attack surface exploited by cyber threat actors.
- With expanded cyber threat detection automation and analysis, reduces state agency 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).
- Enhances the Cal-CSIC's ability to support unserved/underserved populations.

Cons

- Increase in General Fund expenditures.

Alternative 2: Approve funding to maintain only the existing level of service.

Pros

- Maintains existing resources.
- Limits General Fund commitments and maintains previous investments.
- Cal-CSIC will continue to provide its existing level of service.

Cons

- Severely limits Cal-CSIC's ability to respond to increasing demand for services.
- Increases the cyber risk profile for the state, private sector and critical infrastructure partners.
- Increasing risk that Cal-CSIC will not be able to meet multiple statutory requirements, and/or will have increasingly degraded ability to meet remaining requirements as threat landscape evolves.
- Cal-CSIC will not be able to expand into unserved/underserved populations without making difficult decisions of which critical state services to limit support to.
- 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

Cal OES and CDT will advertise and fill positions. CMD and CHP will advertise for assignment opportunities from within their organizations' existing military personnel and CHP officers, respectively. Upon hiring and assignment to the Cal-CSIC, Cal OES will begin in-processing personnel from each of the four agencies and mandatory personnel training, as appropriate. Onboarding training will be followed by specialized Cybersecurity and Incident Response training.

- Conduct training on standard procedures, automated tools, and cyber incident mobilization training.
- Implement processes to proactively analyze and assess risks based on evolving cyber threats.
- Provide outreach to state agencies to assist with implementing best practices to minimize the impact and severity of cyberattacks.
- Conduct analytics on malicious software to determine the full extent of actual or potential damage it could cause; share the indicators with other agencies to implement blocks and other mitigating steps as necessary to prevent spread of the attack through similar methods.
- Respond on-site with highly skilled, trained, and experienced cybersecurity analysts and law enforcement personnel necessary to stop an active attack, pull analytics and share with other agencies, and for law enforcement cyber personnel to conduct forensics necessary to prosecute cyber criminals.

H. Supplemental Information

No supplemental information.

I. Recommendation

Approve $28.7 million General Fund ongoing and 17 positions to continue limited-term resources authorized in 2020-21 (including 23 of the 24 previously authorized positions) and enhance resources to support the responsibilities of the Cal-CSIC. These resources will allow the Cal-CSIC to lead state efforts to identify and mitigate current and ever-evolving cyber threats, including providing enhanced (1) threat detection, assessment, and research; (2) gap testing and remediation; and (3) incident analysis and response.

BCP Fiscal Detail Sheet

BCP Title: California Cybersecurity Integration Center

BR Name: 0690-019-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 - Permanent	0	1,398	1,398	1,398	1,398	1,398
Salaries and Wages Overtime/Other	0	91	91	91	91	91
Total Salaries and Wages	**$0**	**$1,489**	**$1,489**	**$1,489**	**$1,489**	**$1,489**
Total Staff Benefits	0	820	820	820	820	820
Total Personal Services	**$0**	**$2,309**	**$2,309**	**$2,309**	**$2,309**	**$2,309**

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
5301 - General Expense	0	240	240	240	240	240
5302 - Printing	0	20	20	20	20	20
5304 - Communications	0	120	120	120	120	120
5306 - Postage	0	20	20	20	20	20
5320 - Travel: In-State	0	100	100	100	100	100
5322 - Training	0	40	40	40	40	40
5324 - Facilities Operation	0	260	260	260	260	260
5326 - Utilities	0	20	20	20	20	20
5340 - Consulting and Professional Services - External	0	5,600	5,600	5,600	5,600	5,600
5346 - Information Technology	0	4,943	4,896	4,896	4,896	4,896
539X - Other	0	1,910	1,910	1,910	1,910	1,910
Total Operating Expenses and Equipment	**$0**	**$13,273**	**$13,226**	**$13,226**	**$13,226**	**$13,226**

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**	**$15,582**	**$15,535**	**$15,535**	**$15,535**	**$15,535**

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	15,582	15,535	15,535	15,535	15,535
Total State Operations Expenditures	**$0**	**$15,582**	**$15,535**	**$15,535**	**$15,535**	**$15,535**
Total All Funds	**$0**	**$15,582**	**$15,535**	**$15,535**	**$15,535**	**$15,535**

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	15,582	15,535	15,535	15,535	15,535
9900100 - Administration	0	672	672	672	672	672
9900200 - Administration - Distributed	0	-672	-672	-672	-672	-672
Total All Programs	**$0**	**$15,582**	**$15,535**	**$15,535**	**$15,535**	**$15,535**

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
VR00 - Various	0	1,489	1,489	1,489	1,489	1,489
Total Salaries and Wages	**$0**	**$1,489**	**$1,489**	**$1,489**	**$1,489**	**$1,489**

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	182	182	182	182	182
5150450 - Medicare Taxation	0	22	22	22	22	22
5150500 - OASDI	0	92	92	92	92	92
5150630 - Retirement - Public Employees - Miscellaneous	0	401	401	401	401	401
5150900 - Staff Benefits - Other	0	123	123	123	123	123
Total Staff Benefits	**$0**	**$820**	**$820**	**$820**	**$820**	**$820**

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**	**$2,309**	**$2,309**	**$2,309**	**$2,309**	**$2,309**

BCP Fiscal Detail Sheet

BCP Title: California Cybersecurity Integration Center

BR Name: 0690-100-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
Positions - Permanent	0.0	14.0	14.0	14.0	14.0	14.0
Total Positions	**0.0**	**14.0**	**14.0**	**14.0**	**14.0**	**14.0**
Salaries and Wages Earnings - Permanent	0	1,654	1,654	1,654	1,654	1,654
Total Salaries and Wages	**$0**	**$1,654**	**$1,654**	**$1,654**	**$1,654**	**$1,654**
Total Staff Benefits	0	906	906	906	906	906
Total Personal Services	**$0**	**$2,560**	**$2,560**	**$2,560**	**$2,560**	**$2,560**

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	4,804	4,804	4,804	4,804	4,804
539X - Other	0	267	267	267	267	267
Total Operating Expenses and Equipment	**$0**	**$5,071**	**$5,071**	**$5,071**	**$5,071**	**$5,071**

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**	**$7,631**	**$7,631**	**$7,631**	**$7,631**	**$7,631**

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	7,631	7,631	7,631	7,631	7,631

Fund Source	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
Total State Operations Expenditures	**$0**	**$7,631**	**$7,631**	**$7,631**	**$7,631**	**$7,631**
Total All Funds	**$0**	**$7,631**	**$7,631**	**$7,631**	**$7,631**	**$7,631**

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	7,631	7,631	7,631	7,631	7,631
Total All Programs	**$0**	**$7,631**	**$7,631**	**$7,631**	**$7,631**	**$7,631**

Personal Services Details

Positions

Positions	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
VR00 - Various	0.0	14.0	14.0	14.0	14.0	14.0
Total Positions	**0.0**	**14.0**	**14.0**	**14.0**	**14.0**	**14.0**

Salaries and Wages

Salaries and Wages	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
VR00 - Various	0	1,654	1,654	1,654	1,654	1,654
Total Salaries and Wages	**$0**	**$1,654**	**$1,654**	**$1,654**	**$1,654**	**$1,654**

Staff Benefits

Staff Benefits	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
5150450 - Medicare Taxation	0	24	24	24	24	24
5150500 - OASDI	0	103	103	103	103	103
5150630 - Retirement - Public Employees - Miscellaneous	0	529	529	529	529	529
5150900 - Staff Benefits - Other	0	250	250	250	250	250
Total Staff Benefits	**$0**	**$906**	**$906**	**$906**	**$906**	**$906**

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**	**$2,560**	**$2,560**	**$2,560**	**$2,560**	**$2,560**

BCP Fiscal Detail Sheet

BCP Title: California Cybersecurity Integration Center

BR Name: 2720-026-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
Positions - Permanent	0.0	-1.0	-1.0	-1.0	-1.0	-1.0
Total Positions	**0.0**	**-1.0**	**-1.0**	**-1.0**	**-1.0**	**-1.0**
Salaries and Wages Earnings - Permanent	0	384	384	384	384	384
Total Salaries and Wages	**$0**	**$384**	**$384**	**$384**	**$384**	**$384**
Total Staff Benefits	0	363	363	363	363	363
Total Personal Services	**$0**	**$747**	**$747**	**$747**	**$747**	**$747**

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
5301 - General Expense	0	102	102	102	102	102
Total Operating Expenses and Equipment	**$0**	**$102**	**$102**	**$102**	**$102**	**$102**

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**	**$849**	**$849**	**$849**	**$849**	**$849**

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	849	849	849	849	849
Total State Operations Expenditures	**$0**	**$849**	**$849**	**$849**	**$849**	**$849**

Fund Source	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
Total All Funds	**$0**	**$849**	**$849**	**$849**	**$849**	**$849**

Program Summary

Program Funding

Program Funding	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
2050010 - Ground Operations	0	849	849	849	849	849
Total All Programs	**$0**	**$849**	**$849**	**$849**	**$849**	**$849**

Personal Services Details

Positions

Positions	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
VR00 - Various	0.0	-1.0	-1.0	-1.0	-1.0	-1.0
Total Positions	**0.0**	**-1.0**	**-1.0**	**-1.0**	**-1.0**	**-1.0**

Salaries and Wages

Salaries and Wages	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
VR00 - Various	0	384	384	384	384	384
Total Salaries and Wages	**$0**	**$384**	**$384**	**$384**	**$384**	**$384**

Staff Benefits

Staff Benefits	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
5150900 - Staff Benefits - Other	0	363	363	363	363	363
Total Staff Benefits	**$0**	**$363**	**$363**	**$363**	**$363**	**$363**

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**	**$747**	**$747**	**$747**	**$747**	**$747**

BCP Fiscal Detail Sheet

BCP Title: California Cybersecurity Integration Center

BR Name: 7502-005-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 - Permanent	0	821	821	821	821	821
Total Salaries and Wages	**$0**	**$821**	**$821**	**$821**	**$821**	**$821**
Total Staff Benefits	0	443	443	443	443	443
Total Personal Services	**$0**	**$1,264**	**$1,264**	**$1,264**	**$1,264**	**$1,264**

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
5301 - General Expense	0	12	12	12	12	12
5302 - Printing	0	6	6	6	6	6
5304 - Communications	0	12	12	12	12	12
5320 - Travel: In-State	0	36	36	36	36	36
5322 - Training	0	60	60	60	60	60
5324 - Facilities Operation	0	78	78	78	78	78
5340 - Consulting and Professional Services - External	0	6	6	6	6	6
5342 - Departmental Services	0	224	224	224	224	224
5346 - Information Technology	0	18	18	18	18	18
Total Operating Expenses and Equipment	**$0**	**$452**	**$452**	**$452**	**$452**	**$452**

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**	**$1,716**	**$1,716**	**$1,716**	**$1,716**	**$1,716**

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	1,716	1,716	1,716	1,716	1,716
Total State Operations Expenditures	**$0**	**$1,716**	**$1,716**	**$1,716**	**$1,716**	**$1,716**
Total All Funds	**$0**	**$1,716**	**$1,716**	**$1,716**	**$1,716**	**$1,716**

Program Summary

Program Funding

Program Funding	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
6230 - Department of Technology	0	1,716	1,716	1,716	1,716	1,716
Total All Programs	**$0**	**$1,716**	**$1,716**	**$1,716**	**$1,716**	**$1,716**

Personal Services Details

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	125	125	125	125	125
5150450 - Medicare Taxation	0	12	12	12	12	12
5150500 - OASDI	0	51	51	51	51	51
5150600 - Retirement - General	0	255	255	255	255	255
Total Staff Benefits	**$0**	**$443**	**$443**	**$443**	**$443**	**$443**

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**	**$443**	**$443**	**$443**	**$443**	**$443**

BCP Fiscal Detail Sheet

BCP Title: California Cybersecurity Integration Center

BR Name: 7502-039-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
Positions - Permanent	0.0	3.0	3.0	3.0	3.0	3.0
Total Positions	**0.0**	**3.0**	**3.0**	**3.0**	**3.0**	**3.0**
Salaries and Wages Earnings - Permanent	0	393	393	393	393	393
Total Salaries and Wages	**$0**	**$393**	**$393**	**$393**	**$393**	**$393**
Total Staff Benefits	0	221	221	221	221	221
Total Personal Services	**$0**	**$614**	**$614**	**$614**	**$614**	**$614**

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
5301 - General Expense	0	1,030	1,030	1,030	1,030	1,030
Total Operating Expenses and Equipment	**$0**	**$1,030**	**$1,030**	**$1,030**	**$1,030**	**$1,030**

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**	**$1,644**	**$1,644**	**$1,644**	**$1,644**	**$1,644**

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	1,644	1,644	1,644	1,644	1,644
Total State Operations Expenditures	**$0**	**$1,644**	**$1,644**	**$1,644**	**$1,644**	**$1,644**

Fund Source	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
Total All Funds	**$0**	**$1,644**	**$1,644**	**$1,644**	**$1,644**	**$1,644**

Program Summary

Program Funding

Program Funding	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
6230 - Department of Technology	0	1,644	1,644	1,644	1,644	1,644
Total All Programs	**$0**	**$1,644**	**$1,644**	**$1,644**	**$1,644**	**$1,644**

Personal Services Details

Positions

Positions	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
VR00 - Various	0.0	3.0	3.0	3.0	3.0	3.0
Total Positions	**0.0**	**3.0**	**3.0**	**3.0**	**3.0**	**3.0**

Salaries and Wages

Salaries and Wages	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
VR00 - Various	0	393	393	393	393	393
Total Salaries and Wages	**$0**	**$393**	**$393**	**$393**	**$393**	**$393**

Staff Benefits

Staff Benefits	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
5150900 - Staff Benefits - Other	0	221	221	221	221	221
Total Staff Benefits	**$0**	**$221**	**$221**	**$221**	**$221**	**$221**

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**	**$614**	**$614**	**$614**	**$614**	**$614**

BCP Fiscal Detail Sheet

BCP Title: California Cybersecurity Integration Center

BR Name: 8940-024-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 - Permanent	0	685	685	685	685	685
Total Salaries and Wages	**$0**	**$685**	**$685**	**$685**	**$685**	**$685**
Total Staff Benefits	0	546	546	546	546	546
Total Personal Services	**$0**	**$1,231**	**$1,231**	**$1,231**	**$1,231**	**$1,231**

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
5301 - General Expense	0	8	8	8	8	8
5304 - Communications	0	8	8	8	8	8
5320 - Travel: In-State	0	16	16	16	16	16
5322 - Training	0	8	8	8	8	8
5326 - Utilities	0	16	16	16	16	16
5368 - Non-Capital Asset Purchases - Equipment	0	23	6	6	6	6
539X - Other	0	8	8	8	8	8
Total Operating Expenses and Equipment	**$0**	**$87**	**$70**	**$70**	**$70**	**$70**

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**	**$1,318**	**$1,301**	**$1,301**	**$1,301**	**$1,301**

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	1,318	1,301	1,301	1,301	1,301
Total State Operations Expenditures	**$0**	**$1,318**	**$1,301**	**$1,301**	**$1,301**	**$1,301**
Total All Funds	**$0**	**$1,318**	**$1,301**	**$1,301**	**$1,301**	**$1,301**

Program Summary

Program Funding

Program Funding	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
6911035 - Military Civil Support	0	1,318	1,301	1,301	1,301	1,301
Total All Programs	**$0**	**$1,318**	**$1,301**	**$1,301**	**$1,301**	**$1,301**

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
7748 - E7 (Eff. 07-01-2023)	0	87	87	87	87	87
7749 - E6 (Eff. 07-01-2023)	0	230	230	230	230	230
8368 - W2 (Eff. 07-01-2023)	0	183	183	183	183	183
9167 - O2 (Eff. 07-01-2023)	0	185	185	185	185	185
Total Salaries and Wages	**$0**	**$685**	**$685**	**$685**	**$685**	**$685**

Staff Benefits

Staff Benefits	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
5150150 - Dental Insurance	0	1	1	1	1	1
5150210 - Disability Leave - Nonindustrial	0	39	39	39	39	39
5150350 - Health Insurance	0	205	205	205	205	205
5150450 - Medicare Taxation	0	10	10	10	10	10
5150500 - OASDI	0	45	45	45	45	45
5150600 - Retirement - General	0	213	213	213	213	213
5150800 - Workers' Compensation	0	33	33	33	33	33
Total Staff Benefits	**$0**	**$546**	**$546**	**$546**	**$546**	**$546**

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**	**$1,231**	**$1,231**	**$1,231**	**$1,231**	**$1,231**