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

Fiscal Year	Business Unit	Department	Priority No.
2023-24	0690, 7502, 8940	Office of Emergency Services, Department of Technology, and Military Department,	

Budget Request Name	Program	Subprogram
0690-029-BCP-2023-GB 7502-031-BCP-2023-GB 8940-015-BCP-2023-GB	0380 - Emergency Management Services, 6230 – Department of Technology, and 6911 - National Guard	

Budget Request Description
School Cybersecurity (AB 2355)

Budget Request Summary
The Office of Emergency Services (Cal OES), California Department of Technology (CDT), and California Military Department (CMD) jointly request 17 positions (7 positions for Cal OES and 5 positions each for CDF and CMD)—authorized for four years (2023-24 through 2026-27), $5,355,000 General Fund in 2023-24 ($3,401,000 for Cal OES, $1,032,000 for CDT, and $922,000 for CMD), and $3,901,000 each year in 2024-25 through 2026-27 ($1,958,000 for Cal OES, $1,032,000 for CDT, and $911,000 for CMD) to implement Chapter 498, Statutes of 2022 (AB 2355).

Requires Legislation	Code Section(s) to be Added/Amended/Repealed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), California Department of Technology (CDT), and California Military Department (CMD) jointly request 17 positions (7 positions for Cal OES and 5 positions each for CDF and CMD)—authorized for four years (2023-24 through 2026-27), $5,355,000 General Fund in 2023-24 ($3,401,000 for Cal OES, $1,032,000 for CDT, and $922,000 for CMD), and $3,901,000 each year in 2024-25 through 2026-27 ($1,958,000 for Cal OES, $1,032,000 for CDT, and $911,000 for CMD) to implement Chapter 498, Statutes of 2022 (AB 2355).

B. Background/History

Legal Authorities

In 2018, the California Cyber Security Center (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.

Chapter 498, Statutes of 2022 (AB 2355) requires the following:

- Establishment of a database that tracks reports of cyberattacks submitted by local educational agencies
- Requires an annual report to the Governor and the relevant policy committees of the Legislature including:
    - A summary of the types and number of cyberattacks on local educational agencies
    - A summary of the types and number of data breaches affecting local educational agencies that have been reported to the Attorney General
    - Any "activities" provided by Cal-CSIC to prevent cyberattacks or data breaches of a local educational agency
- Support provided by the Cal-CSIC following a cyberattack or data breach of a local educational agency

Current Law

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.

AB 2355

AB 2355 requires school districts (LEAs), county offices of education (COOEs), and charter schools to report any cyberattack impacting more than 500 pupils or personnel to the Cal-CSIC. Further, AB 2355 requires a database be established to track reports of cyberattacks submitted by LEAs and for an annual report to be submitted by January 1st to the Governor and relevant policy committees of the Legislature.

The Cal-CISC has generally been available and responsive to any entity in the state requesting assistance. However, since its inception, the Cal-CSIC has received very limited requests or reports from LEAs. LEAs present a distinctly different type of entity in terms of incident response than state agencies or larger local government organizations such as counties. LEAs generally have very limited IT or cybersecurity resources, maintain potentially sensitive records for many minors, and often do not have consistent, standing relationships with external cybersecurity support entities (consultancies, cyber insurance, federal law enforcement).

Even large, urban LEAs are vulnerable. In 2022, after Los Angeles Unified School District suffered a ransomware attack, they reached out to the Cal-CSIC on several levels for support. However, the Cal-CSIC's response was complicated by a limited understanding by local officials of the Cal-CSIC's role, multiple overlapping communication channels, and ad-hoc coordination between state agencies. All this could be improved with resources dedicated to LEA support, through expanded Cal-CSIC capability to customize operations to address unique LEA needs.

Cal-CSIC has been concerned about the vulnerability of local educational agencies to cyberattack even before AB 2355. That area is an important part of our overall mission, and the California Cybersecurity Task Force Cal OES oversees includes an active Workforce Development and Education committee with participants from local educational agencies. Despite this engagement, K-12 is an area the Cal-CSIC is still trying to increase outreach to, and that effort is limited by the resources of the Cal-CSIC and the all-volunteer Task Force.

Analysis of Problem

Resource History
(Dollars in thousands)

Program Budget	PY – 4	PY – 3	PY – 2	PY-1	PY	CY
Authorized Expenditures	0	0	$7,585	$8,084	$8,084	$8,084
Actual Expenditures	0	0	$7,585	$8,084	$8,084	$8,084
Revenues	0	0	0	0	0	0
Authorized Positions	4	4	6	30	30	30
Filled Positions	3	4	3	7	19	22
Vacancies	1	0	3	23	11	8

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. 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 AB 2355, additional resources would be needed.

Absent an increase in reporting or requests for assistance, this bill would result in costs of $951,000 and three ITS-II positions. However, CalOES anticipates a 100 percent increase of reporting and exponential increase in requests for assistance resulting in the need for 17 positions and $5,355,000 General Fund in 2023-245 and $3,901,000 each year in 2024-25 through 2026-27 to support increased support for the Cal-CSIC to execute AB 2355 requirements. Resources are requested for a four-year period because AB 2355 includes a section repealing its provisions as of January 1, 2027.

To enhance mutual cyber aid and incident response for education sector partners, the Cal-CSIC will be establishing a reporting mechanism for all California educational institutions as well as cyber threat intelligence sharing and evaluating cyber readiness. With the positions requested, the Cal-CSIC could provide on-site incident response to any educational institution in the State of California, if requested. This effort would allow the Cal-CSIC to work in real-time with 58 counties, 1,021 school districts, over 10,500 schools, to protect over 5,892,300 students. The focal point of this additional service would be incident reporting by educational institutions, promote proper cyber hygiene for school networks, and provide vulnerability detection and mitigation services by Cal-CSIC cyber professionals.

It is estimated in 2022 that on average 30,000 websites are hacked every day and that companies fall victim to a cyberattack every 39 seconds. Regulations for cybersecurity around school districts is virtually non-existent at both the state and federal level. Due to the lack of cybersecurity controls, educational institutions are easy targets for cyberattacks, especially ransomware. In 2021, 455 cyber incidents occurred in the education sector, infecting a total of 1,043 schools with ransomware in the United States. In a total of 17 major industries in the United States, the education industry ranked last in cyber security preparedness and awareness. Of the schools impacted by ransomware, 43 percent had student and education staff records compromised, as well as dissertation materials and exam results. Educational data is profitable to cyber bad actors, as education records and exam answer keys can sell for $265 per record on the Dark Web.

To complicate matters further, most school district administrations don't have the proper funding or staff to support a cybersecurity program to protect student data. In a recent IBM Education Ransomware Study of 1,000 educators and 200 administrators, most respondents indicated that their district was not ready to deal with future cyberattacks; 54 percent of educators have no basic cybersecurity awareness training, 61 percent were unaware if the district had cyber insurance, and 54percent responded that funding and budget issues were the biggest barriers for establishing a cybersecurity program. Due to a lack of cybersecurity awareness, it is estimated that 87% of all education institutions have experienced at least one successful cyberattack and approximately 30% of users in the education industry have fallen victim to a phishing email.

Analysis of Problem

AB 2355 requires the establishment of a data system to support the reporting of LEA cyberattacks to the Cal-CSIC. While the Cal-CSIC currently keeps track of all incidents reported to them including the type of incident, reporting party, incident details, and the Cal-CSIC response actions, this law will increase the data received, stored, and analyzed by the Cal CSIC. Although, this AB 2355 does not include "data breach" as part of the definition of a "cyberattack," to avoid confusing and redundant notification requirements cyberattacks as defined are likely to overlap with data breaches. The Attorney General is required to share sample copies of data breach notifications received from LEAs, excluding any personally identifiable information but will require additional workload from the Cal-CSIC to reconcile LEA reports with events detected through our existing cybersecurity monitoring capabilities.

Funding for automated solutions such as security information and event management (SIEM) systems will allow the capture and efficient management of a much broader scale of cyberattack reporting. Using such systems would require Cal-CSIC to directly engage with each local educational agency and establish data sharing agreements and software licensing, help with software installation/configuration, and integrate those SIEM elements into Cal-CSIC's architecture. Cal-CSIC is already accomplishing this with many entities across the state, but mostly on a voluntary basis. While Cal-CSIC has existing solutions for this type of engagement, this bill could significantly increase the scale of that work.

Cal-CSIC is implementing case management systems in addition to existing event monitoring systems which will help us scale up response capabilities. Reporting entities will have to navigate to and fill out their own incident forms. It would be incumbent on each responsible entity to do their own reporting into our platform without additional Cal-CSIC resources to broaden outreach. Even with these software solutions, event reporting thresholds still need to be defined and resources prioritized so the utility of these systems can be maximized. If incident reporting drastically increases, Cal-CSIC will need to make decisions about how to triage, categorize, and prioritize the influx of data which will focus our efforts on the subset of cases we perceive to be the highest priority. Software alone will not solve this problem – Cal-CSIC personnel will need to analyze the data, communicate with reporting entities, and interpret findings. The less defined the reporting requirements are, the more analytic, interpretive, and decision-making burden shifts to Cal-CSIC staff.

As Cal-CSIC and CMD are already monitoring large volumes of data which identify incidents that are not self-reported by affected entities, AB 2355's much broader criteria, could drastically increase Cal-CSIC's processing burden for low-impact events, reducing our ability to adequately address high-impact events absent additional resources.

In 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.

Analysis of Problem

Specifically, this request is seeking the following:

Agency	Item	Justification	Quantity	Classification Requested
OES	Attorney or Attorney III	Staff attorney to advise on information sharing and coordination between Cal-CSIC and DOJ	1	Attorney III
OES	AGPA policy analyst and additional legislative support/analyst	To interpret bill requirements, work with Legislative and External Affairs in determining LEA needs and performing outreach, assemble cost analysis and submit BCP input	2	Assistant Government Program Analyst (AGPA)
CDT	ITS-I System Administrator	ITS-I Additional system administrators to support partner integrator and customer support specialist	2	Information Technology Specialist I (ITS-I)
CDT	ITS-II Database administrator	To manage database to support AB-2355 and assist with system administration of Cal-CSIC systems	1	Information Technology Specialist II (ITS-II)
CDT	ITS-II SIEM/SharePoint administrator	For case management system and/or SEIM	2	Information Technology Specialist II (ITS-II)
CMD	CMD [E5-W2] (1-2)	Ops requirements: we would need additional incident responders to support this effort	2	CMD SAD W2
CMD	CMD/SAD E-5/W-3 (Forensic Analyst)	Ops requirements: we would need additional forensics analyst to support this effort; the State Active Duty personnel come with a wide range of skills and knowledge, most require little training and hit the ground running	2	CMD SAD W-3
CMD	CMD/SAD E-5/W-3 (Incident Responder)	Ops requirements: we would need additional incident	1	CMD SAD W-3

		responders to support this effort; the State Active Duty personnel come with a wide range of skills and knowledge		
OES	ITS III (Incident Responder)	Ops requirements: we would need additional incident responders to support this effort;	1	Information Technology Specialist III (ITS-III)
OES	ITS II (Cyber Defense Analyst)	Ops requirements: we would need additional cyber defense analyst to support this effort;	2	Information Technology Specialist II (ITS-II)
OES	ITS III (Forensics Analyst – Senior Examiner)	Ops requirements: we would need additional forensics analyst to support this effort;	1	Information Technology Specialist III (ITS-III)

Estimated Software Costs to Cal-CSIC of AB-2355 (IT):

Item	Justification	Cost
Acquire/add to case management system and/or SEIM	$650,000 to acquire/add to case management system and/or SEIM	$ 650,000
DomainTools License	For Ops and CTI requirements: used during incident response and CTI investigations	$ 26,250
GroupSense	Used by Ops	$ 150,000
Axiom (2)	Ops requirements: licenses used for forensics analysis during incident response	$ 10,728
Forensics hardware & licenses	Ops requirements: would need additional hardware and software to support incident response, and any proactive cybersecurity assessments	$ 225,000
Kaseware license per each new employee for this requirement of the bill	Ops requirements: Require additional licenses to support the incident responders dedicated for the effort	$ 4,800
Ops Zbook per employee	Ops requirements: each additional Cyber Ops employee supporting this effort would need one	$ 20,700

Pure Signal Recon (Augury) License	Ops requirements: used during incident response and proactive cybersecurity assessments, its used for looking at NetFlow (communications) between the entity and outside world, it's a great resource to identify presence of malicious activity	$ 60,000
Recorded Future License	Ops requirements: used during incident response and proactive cybersecurity assessments, its used to provide the analyst and incident responders with context and intel when looking up artifacts, and indicators of compromise	$ 200,000
Tenable Nessus Licenses (Vuln scanner)	Ops requirements: would need additional software licenses to support proactive cybersecurity assessments, and vulnerability scans during incident response	$ 76,875
	Totals:	**$1,424,353**

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. This is especially true for local educational agencies, many of which are under-resourced generally and these capability gaps are particularly acute in cybersecurity.

E. Outcomes and Accountability

- April 15, 2023 – Begin advanced recruitment for growth positions
- July 1, 2023 – Complete any necessary Inter-Agency Agreements between Cal OES and other agencies (CMD and CDT), begin onboarding staff; initiate security clearance process and conduct onboard training.
- Ongoing/Continuing:
  - Continue and expand training on standard procedures, automated tools, and cyber incident mobilization training
  - Continue and expand specialized individual and team Cybersecurity Incident Response training
  - Grow processes to proactively analyze and assess risks based on evolving cyber threats.
  - Provide outreach to local educational 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.

F. Analysis of All Feasible Alternatives

Alternative 1: Approve 17 positions (7 positions for Cal OES and 5 positions each for CDF and CMD)—authorized for four years (2023-24 through 2026-27), $5,355,000 General Fund in 2023-24 ($3,401,000 for Cal OES, $1,032,000 for CDT, and $922,000 for CMD), and $3,901,000 each year in 2024-25 through 2026-27 ($1,958,000 for Cal OES, $1,032,000 for CDT, and $911,000 for CMD) to implement Chapter 498, Statutes of 2022 (AB 2355).

Pros:

- Ensure continuation of initial state investment in cybersecurity and statutory requirements.
- Expands CA'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 education institutions, 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.
- The Cal-CSIC will continue to fall behind steady and increasing demand for services if we underestimated the rate of demand increase.
- The Cal-CSIC may not be able to accomplish some statutory requirements in AB 2355.
- Inability to fill all positions in a timely manner.

Alternative 2: Deny this proposal.

Pros:

- Limits General Fund commitments.

Cons:

- Severely limits Cal-CSIC's ability to respond to increasing demand for services by education institutions outlined in AB 2355.
- Increases the cyber risk profile for the state and education partners.

- Increasing risk that Cal-CSIC will not be able to meet the statutory requirements of AB 2355, 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 will advertise and fill positions. CMD will advertise for assignment opportunities from within their organizations' existing military personnel. Upon hiring and assignment to the Cal-CSIC, Cal OES will begin in-processing personnel from each of the agencies and mandatory personnel training, as appropriate. Onboarding training will be followed by specialized Cybersecurity and Incident Response training. Following training, Cal CSIC will implement the following:

- Implement processes to proactively analyze and assess risks based on evolving cyber threats.
- Provide outreach to LEAs 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 at school sites 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 17 positions (7 positions for Cal OES and 5 positions each for CDF and CMD)—authorized for four years (2023-24 through 2026-27), $5,355,000 General Fund in 2023-24 ($3,401,000 for Cal OES, $1,032,000 for CDT, and $922,000 for CMD), and $3,901,000 each year in 2024-25 through 2026-27 ($1,958,000 for Cal OES, $1,032,000 for CDT, and $911,000 for CMD) to implement Chapter 498, Statutes of 2022 (AB 2355).

BCP Fiscal Detail Sheet

BCP Title: School Cybersecurity (AB 2355)

BR Name: 0690-029-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	7.0	7.0	7.0	7.0	0.0
Total Positions	**0.0**	**7.0**	**7.0**	**7.0**	**7.0**	**0.0**
Salaries and Wages Earnings - Permanent	0	752	752	752	752	0
Total Salaries and Wages	**$0**	**$752**	**$752**	**$752**	**$752**	**$0**
Total Staff Benefits	0	437	437	437	437	0
Total Personal Services	**$0**	**$1,189**	**$1,189**	**$1,189**	**$1,189**	**$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
5301 - General Expense	0	84	84	84	84	0
5302 - Printing	0	7	7	7	7	0
5304 - Communications	0	42	42	42	42	0
5306 - Postage	0	7	7	7	7	0
5320 - Travel: In-State	0	35	35	35	35	0
5322 - Training	0	14	14	14	14	0
5324 - Facilities Operation	0	91	91	91	91	0
5326 - Utilities	0	7	7	7	7	0
5346 - Information Technology	0	1,537	94	94	94	0
539X - Other	0	388	388	388	388	0
Total Operating Expenses and Equipment	**$0**	**$2,212**	**$769**	**$769**	**$769**	**$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**	**$3,401**	**$1,958**	**$1,958**	**$1,958**	**$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	3,401	1,958	1,958	1,958	0
Total State Operations Expenditures	**$0**	**$3,401**	**$1,958**	**$1,958**	**$1,958**	**$0**
Total All Funds	**$0**	**$3,401**	**$1,958**	**$1,958**	**$1,958**	**$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	3,401	1,958	1,958	1,958	0
9900100 - Administration	0	339	339	339	339	0
9900200 - Administration - Distributed	0	-339	-339	-339	-339	0
Total All Programs	**$0**	**$3,401**	**$1,958**	**$1,958**	**$1,958**	**$0**

Personal Services Details

Positions

Positions	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
1414 - Info Tech Spec II	0.0	2.0	2.0	2.0	2.0	0.0
1415 - Info Tech Spec III	0.0	2.0	2.0	2.0	2.0	0.0
5393 - Assoc Govtl Program Analyst	0.0	2.0	2.0	2.0	2.0	0.0
5795 - Atty III	0.0	1.0	1.0	1.0	1.0	0.0
Total Positions	**0.0**	**7.0**	**7.0**	**7.0**	**7.0**	**0.0**

Salaries and Wages

Salaries and Wages	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
1414 - Info Tech Spec II	0	222	222	222	222	0
1415 - Info Tech Spec III	0	244	244	244	244	0
5393 - Assoc Govtl Program Analyst	0	149	149	149	149	0
5795 - Atty III	0	137	137	137	137	0
Total Salaries and Wages	**$0**	**$752**	**$752**	**$752**	**$752**	**$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	98	98	98	98	0
5150450 - Medicare Taxation	0	11	11	11	11	0
5150500 - OASDI	0	47	47	47	47	0
5150630 - Retirement - Public Employees - Miscellaneous	0	215	215	215	215	0
5150900 - Staff Benefits - Other	0	66	66	66	66	0
Total Staff Benefits	**$0**	**$437**	**$437**	**$437**	**$437**	**$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**	**$1,189**	**$1,189**	**$1,189**	**$1,189**	**$0**

BCP Fiscal Detail Sheet

BCP Title: California Cybersecurity Integration Center (AB 2355)

BR Name: 7502-031-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
Positions - Permanent	0.0	5.0	5.0	5.0	5.0	0.0
Total Positions	**0.0**	**5.0**	**5.0**	**5.0**	**5.0**	**0.0**
Salaries and Wages Earnings - Permanent	0	521	521	521	521	0
Total Salaries and Wages	**$0**	**$521**	**$521**	**$521**	**$521**	**$0**
Total Staff Benefits	0	281	281	281	281	0
Total Personal Services	**$0**	**$802**	**$802**	**$802**	**$802**	**$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
5301 - General Expense	0	10	10	10	10	0
5304 - Communications	0	5	5	5	5	0
5320 - Travel: In-State	0	5	5	5	5	0
5324 - Facilities Operation	0	50	50	50	50	0
5342 - Departmental Services	0	135	135	135	135	0
5346 - Information Technology	0	25	25	25	25	0
Total Operating Expenses and Equipment	**$0**	**$230**	**$230**	**$230**	**$230**	**$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**	**$1,032**	**$1,032**	**$1,032**	**$1,032**	**$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	1,032	1,032	1,032	1,032	0
Total State Operations Expenditures	**$0**	**$1,032**	**$1,032**	**$1,032**	**$1,032**	**$0**
Total All Funds	**$0**	**$1,032**	**$1,032**	**$1,032**	**$1,032**	**$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
6230 - Department of Technology	0	1,032	1,032	1,032	1,032	0
Total All Programs	**$0**	**$1,032**	**$1,032**	**$1,032**	**$1,032**	**$0**

Personal Services Details

Positions

Positions	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
1402 - Info Tech Spec I	0.0	2.0	2.0	2.0	2.0	0.0
1414 - Info Tech Spec II	0.0	3.0	3.0	3.0	3.0	0.0
Total Positions	**0.0**	**5.0**	**5.0**	**5.0**	**5.0**	**0.0**

Salaries and Wages

Salaries and Wages	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
1402 - Info Tech Spec I	0	188	188	188	188	0
1414 - Info Tech Spec II	0	333	333	333	333	0
Total Salaries and Wages	**$0**	**$521**	**$521**	**$521**	**$521**	**$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	79	79	79	79	0
5150450 - Medicare Taxation	0	8	8	8	8	0
5150500 - OASDI	0	32	32	32	32	0
5150600 - Retirement - General	0	162	162	162	162	0
Total Staff Benefits	**$0**	**$281**	**$281**	**$281**	**$281**	**$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**	**$802**	**$802**	**$802**	**$802**	**$0**

BCP Fiscal Detail Sheet

BCP Title: California Cybersecurity Integration Center (AB 2355)

BR Name: 8940-015-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	5.0	5.0	5.0	5.0	0.0
Total Positions	**0.0**	**5.0**	**5.0**	**5.0**	**5.0**	**0.0**
Earnings - Permanent	0	524	524	524	524	0
Total Salaries and Wages	**$0**	**$524**	**$524**	**$524**	**$524**	**$0**
Total Staff Benefits	0	343	343	343	343	0
Total Personal Services	**$0**	**$867**	**$867**	**$867**	**$867**	**$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
5301 - General Expense	0	5	5	5	5	0
5304 - Communications	0	5	5	5	5	0
5320 - Travel: In-State	0	10	10	10	10	0
5322 - Training	0	5	5	5	5	0
5326 - Utilities	0	10	10	10	10	0
5368 - Non-Capital Asset Purchases - Equipment	0	15	4	4	4	0
539X - Other	0	5	5	5	5	0
Total Operating Expenses and Equipment	**$0**	**$55**	**$44**	**$44**	**$44**	**$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**	**$922**	**$911**	**$911**	**$911**	**$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	922	911	911	911	0
Total State Operations Expenditures	**$0**	**$922**	**$911**	**$911**	**$911**	**$0**
Total All Funds	**$0**	**$922**	**$911**	**$911**	**$911**	**$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
6911035 - Military Civil Support	0	922	911	911	911	0
Total All Programs	**$0**	**$922**	**$911**	**$911**	**$911**	**$0**

Personal Services Details

Positions

Positions	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
8367 - W3 (Eff. 07-01-2022)	0.0	2.0	2.0	2.0	2.0	2.0
8368 - W2 (Eff. 07-01-2022)	0.0	2.0	2.0	2.0	2.0	2.0
9166 - O3 (Eff. 07-01-2022)	0.0	1.0	1.0	1.0	1.0	1.0
Total Positions	**0.0**	**5.0**	**5.0**	**5.0**	**5.0**	**5.0**

Salaries and Wages

Salaries and Wages	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
8367 - W3 (Eff. 07-01-2022)	0	218	218	218	218	218
8368 - W2 (Eff. 07-01-2022)	0	196	196	196	196	196
9166 - O3 (Eff. 07-01-2022)	0	110	110	110	110	110
Total Salaries and Wages	**$0**	**$524**	**$524**	**$524**	**$524**	**$524**

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	4	4	4	4	0
5150350 - Health Insurance	0	104	104	104	104	0
5150450 - Medicare Taxation	0	15	15	15	15	0
5150500 - OASDI	0	32	32	32	32	0
5150600 - Retirement - General	0	168	168	168	168	0
5150700 - Unemployment Insurance	0	1	1	1	1	0
5150800 - Workers' Compensation	0	19	19	19	19	0
Total Staff Benefits	**$0**	**$343**	**$343**	**$343**	**$343**	**$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**	**$867**	**$867**	**$867**	**$867**	**$524**