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

Fiscal Year	Business Unit	Department	Priority No.
2023-24	7870	California Victim Compensation Board (CalVCB)	1

Budget Request Name	Program	Subprogram
7870-002-BCP-2023-GB	9900100 Administration	Click or tap here to enter text.

Budget Request Description
Information Technology Staff

Budget Request Summary
The California Victim Compensation Board requests $877,000 Restitution Fund and 4.0 positions in 2023-24 and $789,000 and 4.0 positions in 2024-25 and ongoing to implement and maintain increased cybersecurity capabilities.

Requires Legislation	Code Section(s) to be Added/Amended/Repealed
☐ Yes ☒ No	Click or tap here to enter text.

Does this BCP contain information technology (IT) components? ☒ Yes ☐ No *If yes, departmental Chief Information Officer must sign.*	Department CIO Abdul Shaik	Date 1/10/20223

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. Not Applicable **Project Approval Document:** Not Applicable

Approval Date: Click or tap to enter a 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
Albert Lam	1/10/2023	Natalie Mack	1/10/2023
Department Director	**Date**	**Agency Secretary**	**Date**
Lynda Gledhill	1/10/2023	Justyn Howard	1/10/2023

Department of Finance Use Only

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

PPBA	Date submitted to the Legislature
Mark Jimenez	1/10/2023

A. Budget Request Summary

The California Victim Compensation Board requests $877,000 Restitution Fund and 4.0 positions in 2023-24 and $789,000 and 4.0 positions in 2024-25 and ongoing to implement and maintain increased cybersecurity capabilities.

B. Background/History

Created in 1965, CalVCB plays a vital role in assisting victims of violent crime across the state and helping them recover and restore their lives. CalVCB helps crime victims pay for funerals, medical bills, mental health treatment and relocation costs, as well as provides income replacement for victims and their families (California Government Code §§ 13950 to 13974). As such, it is imperative to have effective security measures and strategies in place to prevent cybercrime and risks to the confidential data of the crime victims, as well as organizational risk management, governance and internal control processes to ensure operational efficiencies and compliance.

In October 2021, the California Department of Technology (CDT) and its Office of Information Security (OIS) released the Governor's multi-year Cyber Information Security Maturity Roadmap called Cal-Secure. Cal-Secure's plan builds on the key objectives of the California Homeland Security Strategy, under which California established a goal to strengthen security and preparedness across cyberspace by enhancing safety and preparedness with state federal, local, tribal, and private sector stakeholders.

Cal-Secure has 29 required capabilities to strengthen the state's security and preparedness across Cyberspace. Of the 29 capabilities, CalVCB has been able to absorb the workload for nine of the capabilities. At the close of each fiscal year, state departments and agencies will be required to attest that they have achieved the required capabilities.

Current Information Technology (IT) Security staffing levels at CalVCB are not adequate to implement and support the cybersecurity requirements of Cal-Secure. CalVCB currently has 1.2 information security staff positions for maintaining the information security program as required under SAM Section 5300.

Analysis of Problem

Resource History
(Dollars in thousands)

Information Technology Security	2017-18 PY – 4	2018-19 PY – 3	2019-20 PY – 2	2020-21 PY-1	2021-22 PY	2022-23 CY
Authorized Expenditures	315	232	255	315	373	1,066
Actual Expenditures	140	180	242	262	TBD	TBD
Revenues	0	0	0	0	0	0
Authorized Positions	1.0	1.0	1.0	1.0	1.2	1.2
Filled Positions	1.0	1.0	1.0	0.5	1.2	1.2
Vacancies	0.0	0.0	0.0	0.5	0.0	TBD

C. State Level Consideration

CalVCB plays a vital role in assisting victims of violent crime across the state and helping them recover and restore their lives. This mission reinforces the Governor's priorities to fight crime, protect Californians and provide the support they need to be healthy and productive. This proposal will enable CalVCB to reduce data security risks while executing departmental statutory functions.

D. Justification

CalVCB requests 4.0 positions and $877,000 in Restitution Fund in FY 2023-24, and $789,000 in Restitution Funds annually starting in FY 2024-25 to improve IT Security, to be in compliance with Cal-Secure, to protect victims of crime's information, and to be compliant with applicable laws, regulations, and directives. Of the 29 capabilities required by Cal-Secure, CalVCB is able to absorb the workload to implement and maintain nine of them. CalVCB is requesting 4.0 IT Security staff to implement and maintain the remaining 20 capabilities that are not absorbable with the current staffing levels.

The status of the 29 required capabilities are illustrated in the table below. Overall, the average coverage of the capabilities is 35%. This means that there are significant staff workloads to expand coverage of most existing solutions so more applicable CalVCB systems are equipped with the required cybersecurity capabilities. In some cases, the existing solutions are technically constrained that they must be replaced with more powerful solutions to handle the processing needs of covering more systems.

Analysis of Problem

#	Capability	Implementation Progress	Resource for Workload
1	Anti-Malware Protection (AMP)	90%	Absorb by existing staff
2	Anti-Phishing Program	50%	Absorb by existing staff
3	Multi-Factor Authentication	20%	Absorb by existing staff
4	Continuous Vulnerability Management	90%	Need new position
5	Asset Management	30%	Need new position
6	Incident Response	20%	Need new position
7	Continuous Patch Management	70%	Absorb by existing staff
8	Privileged Access Management	50%	Need new position
9	Security and Privacy Awareness Training	50%	Absorb by existing staff
10	Security Continuous Monitoring 24x7	10%	Need new position
11	Cloud Security Monitoring	0%	Need new position
12	Data Loss Prevention	20%	Need new position
13	Log Management	30%	Need new position
14	Network Threat Detection	40%	Absorb by existing staff
15	Network Threat Protection	40%	Absorb by existing staff
16	Threat Intelligence Platform	50%	Need new position
17	Application Security	0%	Need new position
18	Operational Technology Security	0%	Need new position
19	Disaster Recovery	86%	Absorb by existing staff
20	Enterprise Sign-On	70%	Need new position
21	Mobile Device Management	50%	Absorb by existing staff
22	Application Development Security	0%	Need new position
23	Application Whitelisting	0%	Absorb by existing staff
24	Software Supply Chain Management	0%	Need new position
25	Identity Lifecycle Management	80%	Need new position
26	Insider Threat Detection	0%	Need new position
27	Network Access Control	50%	Need new position
28	Enterprise Encryption	90%	Need new position
29	Mobile Threat Defense	20%	Absorb by existing staff

This proposal addresses the new workload with 4.0 new positions as outlined below:

Summary of Positions by Classifications		
Classification	**PY**	**Effective Date**
Information Technology Specialist I	1.0	7/1/2023
Information Technology Specialist II	3.0	7/1/2023
Total	**4.0**	

- **Security & Privacy Analyst** (1.0 IT Specialist I)

  The Security and Privacy Analyst (IT Specialist I) will be responsible for developing new and updating existing policies and procedures to incorporate changes associated with the Cal-Secure required capabilities, maintaining the Cal-Secure required capabilities of asset management and software supply chain management, and for the overhead tasks created by the additional requirements. This position will also take over incident response triaging, documentation, and compliance reporting responsibilities from the existing Information Security Section Chief.

  This position requires skills and knowledge in the information security engineering and business technology management domains. To support and maintain the Cal-Secure capabilities for CalVCB, this position's primary duties include (1) analyze and identify security policy needs and gap analysis; (2) audit IT assets to maintain accountability using asset management tools; (3) analyze business impact and exposure of risks for supply chain transactions; (4) investigate security incidents; and (5) assist management with policies and procedures development. The workloads associated with these duties require in-depth understanding of security incident and supply chain risk management. Most of the duties for this position are in the information security domain and typically are not performed by position at the Information Technology Technician or Associate levels. Accordingly, this new position must be at the level of at least Information Technology Specialist I.

Security & Privacy Analyst Workload (1.0 IT Specialist I)

*Workload in hours

Capability Workload	**CY**	**BY**	**BY+1**	**BY+2**	**BY+3**	**BY+4**
5 - Asset Management	0	300	350	350	350	350
6 - Incident Response	0	480	360	360	360	360
24 - Software Supply Chain Management	0	0	240	200	200	200
Additional duties, including policy & procedures for the 29 capabilities	0	870	870	870	870	870
Total, Hours	**0**	**1,650**	**1,820**	**1,780**	**1,780**	**1,780**

- **Infrastructure Security Lead** (1.0 IT Specialist II)

  The Infrastructure Security Lead position will have the responsibility for improving infrastructure security for CalVCB's Compensation and Restitution System (CaRES2)as well as the underlying infrastructure by implementing and integrating new security solutions and expanding coverage of existing infrastructure security solutions. Specifically, this position is responsible for the Cal-Secure capabilities of privileged access management, operational technology security, enterprise sign-on, enterprise encryption, network access control, application security, application development security, and identity lifecycle management.

  This position requires a depth of leadership and expertise in the information security engineering, System Engineering, and Software Engineering domains. To implement and maintain the Cal-Secure capabilities for CalVCB, this position's primary duties include (1) assess and recommend IT solutions; (2) design the architectures and solutions to support security requirements; (3) manage integration of systems; (4) report system security statuses;

and (5) lead and mentor other staff. The workloads associated with these duties require complex, extensive problem and system analysis, and independent problem-solving without established guidance. Accordingly, this new position must be at the level of at least Information Technology Specialist II.

Infrastructure Security Lead (1.0 IT Specialist II)

*Workload in hours

Capability Workload	CY	BY	BY+1	BY+2	BY+3	BY+4
6 - Incident Response	0	174	174	192	192	192
8 - Privileged Access Management	0	0	472	192	192	192
17 - Application Security	0	350	300	300	300	300
18 - Operational Technology Security	0	0	192	192	192	192
20 - Enterprise Sign-On	0	0	60	360	192	192
22 - Application Development Security	0	0	100	80	80	80
25 - Identity Lifecycle Management	0	160	100	100	100	260
27 - Network Access Control	0	440	192	192	192	192
28 - Enterprise Encryption	0	456	192	192	192	192
Additional Duties	0	70	70	70	70	70
Total, Hours	**0**	**1,650**	**1,852**	**1,870**	**1,702**	**1,826**

- **Technical Security & Privacy Engineers** (2.0 IT Specialist II)

  The 2.0 IT Specialist II positions will be responsible for the implementation, maintenance, and management of the department's technical security and privacy solutions.

  Specifically, the first position is responsible for the Cal-Secure capabilities of security continuous monitoring, log management, and software supply chain management. This position will also take over continuous vulnerability management responsibilities from the existing Information Security Officer, who will have increased personnel and project management workload implementing the Cal-Secure capabilities.

  The second position is responsible for the Cal- Secure required capabilities of cloud security monitoring, data loss prevention, threat intelligence platform, and insider threat detection. This position will also take over incident response responsibilities from the existing Information Security Officer.

  These 2.0 positions require a depth of leadership and expertise in the information security engineering and System Engineering domains. To implement and maintain the Cal-Secure capabilities for CalVCB, this position's primary duties include (1) ensure security solutions and technical artifacts are in place throughout all IT systems and platforms; (2) design the architectures and solutions to support security requirements; (3) analyze incident-related data and determine the appropriate response; (4) monitor and assess security controls; and (5) lead and mentor other staff. The workloads associated with these duties require complex, extensive problem and system analysis, and independent problem-solving without established guidance. Accordingly, these two new positions must be at the level of at least Information Technology Specialist II.

Technical Security & Privacy Engineer 1 (1.0 IT Specialist II)

*Workload in hours

Capability	CY	BY	BY+1	BY+2	BY+3	BY+4
4 - Continuous Vulnerability Management	0	1,100	800	800	600	600
10 - Security Continuous Monitoring 24x7	0	0	620	800	1,040	1,040
13 - Log Management	0	520	120	120	120	120
24 - Software Supply Chain Management	0	0	184	24	24	24
Additional Duties	0	70	70	70	70	70
Total, Hours	**0**	**1,690**	**1,794**	**1,814**	**1,854**	**1,854**

Technical Security & Privacy Engineer 2 (1.0 IT Specialist II)

*Workload in hours

Capability Workload	CY	BY	BY+1	BY+2	BY+3	BY+4
6 - Incident Response	0	552	192	192	192	192
10 - Security Continuous Monitoring 24x7	0	0	780	780	940	940
11 - Cloud Security Monitoring	0	512	192	192	192	192
12 - Data Loss Prevention	0	200	176	96	96	96
16 - Threat Intelligence Platform	0	0	460	260	260	260
26 - Insider Threat Detection	0	0	0	256	96	96
Additional Duties	0	70	70	70	70	70
Total, Hours	**0**	**1,334**	**1,870**	**1,846**	**1,846**	**1,846**

E. Outcomes and Accountability

Approval of this request will address CalVCB staffing needs to implement and maintain new cybersecurity solutions and meet Cal-Secure requirements. Accountability will be measured by annual assessment that will be submitted to the California Department of Technology (CDT), and by Independent Security Assessments conducted by the California Military Department every other year. Additionally, progress will also be reported to CDT following the process specified in Statewide Information Management Manual (SIMM) Section 5305.

F. Analysis of All Feasible Alternatives

Alternative 1: Approve California Victim Compensation Board requests $877,000 Restitution Fund and 4.0 positions in 2023-24 and $789,000 in 2024-25 and ongoing to (1) implement and maintain solutions for 6 additional cybersecurity capabilities; (2) expand implementation of 14 existing solutions to cover more applicable CalVCB systems; and (3) implement and maintain relevant policies and procedures.

Pros:

- Enable CalVCB to act on the Governor's directives and implement the Cal-Secure roadmap
- Improve protection of the privacy and security of victim's information significantly
- Mature the cybersecurity posture of CalVCB Systems significantly
- Enhance overall information security and privacy program compliance
- Enable policies and procedures corresponding to cybersecurity capabilities to be documented
- Increase CalVCB's cybersecurity maturity and security assessment scores substantially in future California Military Department (CMD) assessments and other audits

Cons:

- Increased costs to the Restitution Fund
- Requires permanent, ongoing Restitution Fund expenditures

Alternative 2: Approve $674,000 from the Restitution Fund to fund 3.0 permanent positions (at the IT Specialist II level) in 2023-24 and $608,000 ongoing and approve the IT Specialist I position for a limited 2-year term for $203,000 in year 1 and $181,000 in year 2, to address the new requirements from Cal-Secure, implement and maintain new technological solutions, as well as to expand coverage of existing solutions.

Pros:

- Enable CalVCB to act on the Governor's directives and implement the Cal-Secure roadmap
- Improve protection of the privacy and security of victim's information
- Mature the cybersecurity posture of CalVCB Systems
- Enhance overall information security and privacy program compliance
- Increase CalVCB's security assessment scores in future California Military Department (CMD) assessments and other audits
- Require fewer ongoing funding than Alternative 1

Cons:

- Increased costs to the Restitution Fund
- Requires permanent, ongoing Restitution Fund expenditures
- Some policies and procedures for the new capabilities will likely be significantly delayed or outdated

- CalVCB's cybersecurity maturity and audit scores in future information security program audits will be significantly lower due to lack of or outdated policies
- Higher risks associated with supply chain and asset management due to the lack of resource to execute supply-chain transactions, manage supplier relationships, control associated business processes, and to identify and classify entity-owned hardware and software

Alternative 3: Approve only $674,000 from the Restitution Fund to fund 3.0 permanent positions (at the IT Specialist II level) in 2023-24 and $608,000 ongoing to address the new requirements from Cal-Secure, implement and maintain new technological solutions, as well as to expand coverage of existing solutions.

Pros:

- Enable CalVCB to act on the Governor's directives and implement the Cal-Secure roadmap
- Improve protection of the privacy and security of victim's information
- Mature the cybersecurity posture of CalVCB Systems
- Enhance overall information security and privacy program compliance
- Increase CalVCB's security assessment scores in future California Military Department (CMD) assessments
- Require fewer ongoing funding than Alternatives 1 and 2

Cons:

- Increased costs to the Restitution Fund
- Requires permanent, ongoing Restitution Fund expenditures
- Some policies and procedures for the new capabilities will likely be delayed or outdated
- CalVCB's cybersecurity maturity and audit scores in future information security program audits will be significantly lower due to lack of or outdated policies
- Higher risks associated with supply chain and asset management due to the lack of resource to execute supply-chain transactions, manage supplier relationships, control associated business processes, and to identify and classify entity-owned hardware and software

Alternative 4: Do not approve the additional resources requested.

Pros:

- No increased costs to the Restitution Fund

Cons:

- CalVCB will not have the necessary resources to address the new requirements from Cal-Secure
- Privacy and security of victim's information are at significantly high risk of being breached
- CalVCB Systems are significantly more vulnerable to cybersecurity threats

- No improvement to CalVCB's cybersecurity maturity and security assessment scores in future California Military Department (CMD) assessments and other audits
- CalVCB's overall information security and privacy program compliance level will not improve

G. Implementation Plan

CalVCB will hire to fill the additional authorized positions to start in Fiscal Year 2023-24, and once filled, CalVCB will have the capacity to address Cal-Secure required capabilities by implementing new solutions, expanding implementation of existing solutions, and implement relevant policies and procedures.

H. Supplemental Information (*Describe special resources and provide details to support costs including appropriate back up*.)

The Cal-Secure document is available on CDT's website. Specifically, the document may be found at https://cdt.ca.gov/wp-content/uploads/2021/10/Cybersecurity_Strategy_Plan_FINAL.pdf.

Additional context on Cal-Secure is available on the Office of Governor's published news may be found at https://www.gov.ca.gov/2021/10/22/newsom-administration-announces-first-multi-year-cybersecurity-roadmap-to-protect-californians-privacy-and-security/.

The relevant State Administrative Manual (SAM) chapter may be found at https://www.dgs.ca.gov/Resources/SAM/TOC/5300.

The relevant Statewide Information Management Manual (SIMM) is available on CDT's website at https://cdt.ca.gov/policy/simm/.

I. Recommendation

Approve CalVCB's request for $877,000 from the Restitution Fund to fund 4.0 permanent positions in 2023-24 and $789,000 and 4.0 positions ongoing to meet the anticipated workload for implementation and maintenance of cybersecurity capabilities required under Cal-Secure.

BCP Fiscal Detail Sheet

BCP Title: Information Technology Staff

BR Name: 7870-002-BCP-2023-GB

Personal Services	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
Positions - Permanent	0.0	4.0	4.0	4.0	4.0	4.0
Total Positions	**0.0**	**4.0**	**4.0**	**4.0**	**4.0**	**4.0**
Salaries and Wage Earnings - Permanent	0	425	425	425	425	425
Total Salaries and Wages	**$0**	**$425**	**$425**	**$425**	**$425**	**$425**
Total Staff Benefits	0	251	251	251	251	251
Total Personal Services	**$0**	**$676**	**$676**	**$676**	**$676**	**$676**

Operating Expenses and Equipment	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
Operating Expenses and Equipment	0	201	113	113	113	113
Total Operating Expenses and Equipment	**$0**	**$201**	**$113**	**$113**	**$113**	**$113**

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**	**$877**	**$789**	**$789**	**$789**	**$789**

Fund Source

Fund Source	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
State Operations - 0214 - Restitution Fund	0	877	789	789	789	789
Total State Operations Expenditures	**$0**	**$877**	**$789**	**$789**	**$789**	**$789**
Total All Funds	**$0**	**$877**	**$789**	**$789**	**$789**	**$789**