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

Fiscal Year	Business Unit	Department	Priority No.
2023-24	7502	California Department of Technology	7

Budget Request Name	Program	Subprogram
7502-009-BCP-2023-GB	6230	N/A

Budget Request Description
Intrusion Detection & Prevention System

Budget Request Summary
The California Department of Technology requests $2.96 million in General Fund Authority in Fiscal Year 2023-24 to upgrade the State's Intrusion Detection and Intrusion Prevention Systems. In addition, the California Department of Technology also requests $1.93 million in on-going General Fund authority to maintain these systems beginning in Fiscal Year 2024-25. These contemporary system upgrades are necessary for the State to continue to provide a frontline defense against malicious actors.

Requires Legislation	Code Section(s) to be Added/Amended/Repealed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

Does this BCP contain information technology (IT) components? ☒ Yes ☐ No *If yes, departmental Chief Information Officer must sign.*	Department CIO Quentin Wright	Date 9/1/2022

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. N/A **Project Approval Document:** N/A

Approval Date: N/A

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
Brent Horiuchi	12/20/2022	Miles Burnett	12/20/2022
Department Director	**Date**	**Agency Secretary**	**Date**
Liana Bailey-Crimmins	12/20/2022	Amy Tong	12/20/2022

Department of Finance Use Only

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

PPBA	Date submitted to the Legislature
Danielle Brandon	1/10/2023

A. Budget Request Summary

The California Department of Technology (CDT) requests $2.96 million in General Fund (GF) Authority in Fiscal Year (FY) 2023-24 to upgrade the State's Intrusion Detection (IDS) and Intrusion Prevention Systems (IPS). In addition, CDT also requests $1.93 million in on-going GF authority to maintain these systems beginning in FY 2024-25. These contemporary system upgrades and maintenance are necessary for the State to continue to provide a frontline defense against malicious actors.

B. Background/History

Intrusion detection is a critical component for safeguarding the State of California's data and IT infrastructure. CDT has historically deployed security technologies to support the protection requirements of the California Government Enterprise Network (CGEN) and the state entities that comprise its membership. IDS systems were first deployed by the Department in 2001 and IPS systems in 2004.

As the state's data and communication demands have continued to increase, California must increase its network capacity and resiliency to maintain these critical statewide security services. To address this issue, the Office of Information Security (OIS) is submitting this proposal to implement next generation IDS and IPS systems statewide to advance the State's cybersecurity infrastructure. At present, the Federal government, multiple state governments, the top 100 banks, and leading corporations all utilize IPS/IDS systems, further illustrating their importance as an essential frontline Information Technology (IT) security defense. As these systems also represent a fundamental component of California's network-based security, it is imperative that the State continues to invest in these mission-critical systems to ensure that they remain updated in accordance with established IT security practices.

C. State Level Considerations

Public sector leaders must secure the trust and gain the confidence of consumers of government services and information if the state is to continue effectively serving constituents. To ensure trust, the State must safeguard sensitive data through strong privacy and data security practices. Furthermore, departments must be prepared to operate during times of disruption (cyberattacks, natural disasters, unplanned outages, and other events) to mitigate the impact on state business.

By leveraging data resources and analytical capabilities, the state can convert data it already collects into actionable information to make informed policy decisions, administer programs, reduce costs, improve outcomes, and better serve constituents. By making IT systems and transactions secure, departments ensure that the citizens of California can leverage technology with confidence to access the services and information they need. This BCP supports the following goals from the Vision 2023 California Technology Strategic Plan.

Goal 2: Ensure Secure Delivery - Advance the maturity of information security across California government.
1) Protect California's information assets and maximize data access.
2) Develop a robust and collaborative risk reduction strategy.
3) Develop an enterprise approach to security leadership and governance.
4) Improve and invest in security capabilities to protect mission-critical systems and data.
5) Foster a security-minded culture throughout California's workforce.

The second goal and challenge listed in CDT's Strategic Plan (Vision 2023 – California Technology Strategic Plan) is to "Ensure public services are equitable and inclusive." Achieving this requires focus and work that stretches beyond the myriad languages spoken within the State, requires considerations of access and accessibility, and necessitates that technology be simplified as much as possible. CDT works diligently to ensure all services are provided equitably and are accessible to all Californians. While this request does not directly address matters of equity, diversity, or accessibility, the underlying principles listed above are foundational. Additionally, CDT provides underlying support, and delivers technology, to

departments that do address matters of equity such as expanding access to previously marginalized demographics or geographically precluded groups. CDT's Strategic Plan provides the framework for all our service deliveries, and equity is paramount.

D. Justification

To respond to the growing number of cyber incidents, withstand a large-scale cyber-attack, and minimize potential catastrophic consequences, the State must continue to invest and expand its overall statewide IDS and IPS capabilities. Specifically, OIS has identified an increasing demand for network and Internet access, requiring an increase in network capacity. Network security technologies must expand to ensure the security of the state's data and IT infrastructure is not impacted.

State funding for this security capability needs to be linked to the current and future growth of California's comprehensive network. It is a fundamental component of network-based security that the security tools match the network in speed, capacity, and performance. This is a standard practice used by all large enterprise networks. The network security model employed by the State of California has been copied by many of the State's counties and is very similar to Federal guidelines.

These systems have continually provided a critical statewide benefit by serving as a frontline defense against malicious actors, as they are standard tools, widely used for securing large networks. IPS/IDS systems block and detect millions of malicious actions targeting the state's network hourly. These devices were used in detecting and then protecting from attacks on the DMV Motor Voter website, are used to block Russia and China from launching attacks from their home networks and are used to control or limit access via selected high-risk protocols such as Remote Desktop Protocol, Secure Shell, File Transfer protocol and more.

Successfully implementing and funding these next generation security solutions will serve to significantly strengthen the State's technical baseline capabilities, mitigating advanced attacks from new and unknown malicious entities. With the use of the IDS and IPS devices, there will be continued monitoring and blocking of malicious actions on the state's network. Denial of Service attacks can be detected and mitigated, as well as partially providing Domain Name security. The solution will also allow for existing and future security teams to triage and investigate suspected malicious cyber activity and prevent that activity before any large-scale negative consequences are sustained. Blocking on known malicious IP addresses and Domain names is a key element to the state's cyber security posture.

Based on current standard security protocol regarding intrusions, not all security actions result in a logged event. Those that are logged show 11 million attacks per hour blocked at our network edge and another million per hour at the data center edge. We estimate unlogged blocks at about that of the logged blocks or another 11 million per hour. The Network is rapidly expanding throughput, and our security tool must be able to keep up, which is the reason for needing the contemporary IPS equipment. For IDS, we needed greater capacity, but the IDS devices also were end of life and obsolete. As the network grows, so too must our security tools. There is significant risk in forcing the use of an outdated device, including the risk of the device to stop working, causing a weakness in the network edge, and potentially allowing for a security breach.

Using IPS and IDS devices prevents breaches, loss of reputation, and more. It is not possible to quantify the savings of such protection. Typical breaches cost tens of millions of dollars. In 2010, the IPS was used to detect and stop a breach of the Interim Statewide Automated Welfare System (ISAWS) program, which would have exposed 680,000 state of California constituents. Cost of notification per user at that time was $100 per user, thus in 2010 the IPS saved the state $68,000,000. The cost of such a breach today would be three to four times higher. New upgrades to the equipment could potentially be viable for at least five years.

Analysis of Problem

As outlined in Cal Secure, OIS will develop and unify California's diverse, innovative cybersecurity workforce to safeguard the data and systems used to deliver public services. Cal-Secure calls for the collaboration of CDT's Security Operations Center (SOC), Cal-CSIC, and all state entities to tackle threats across the state. The SOC, Cal-CSIC and state entities provide continuous security monitoring of threats at endpoints and on CGEN, dramatically and efficiently improving the state's cybersecurity posture and ability to quickly mitigate cybersecurity risk.

For these specific reasons, CDT is requesting that the State approve this GF request for $2.96 million in FY 2023-24 and $1.93 million in ongoing authority beginning in FY 2024-25 to upgrade and maintain these critical state security systems.

E. Outcomes and Accountability

Through the approval of CDT's GF request to upgrade the State's IDS/IPS and the needed ongoing funds to upgrade/maintain these critical state security systems, the CDT SOC will be able to replace all devices reaching end of life, significantly strengthening the State's technical capabilities, mitigating attacks. The solution will allow for security teams to triage and investigate suspected malicious cyber activity and prevent that activity prior to an incident occurring.

The IDS will be installed by October of 2022. The IPS systems were purchase and are in place now. Funding is needed for future growth and more importantly, yearly maintenance, software, and security updates.

Projected Outcomes

Workload Measure	CY	FY 22-23	FY 23-24	FY 24-25	FY 25-26	FY 26-27
IDS/ IPS upgrades/ maintenance	0	0	100% Upgrade/Replacement of end of life equipment	100% Maintenance	100% Maintenance	100% Maintenance

F. Analysis of All Feasible Alternatives

ALTERNATIVE 1 - Approve CDT's GF request for $2.96 million in FY 2023-24 to upgrade the State's IDS/IPS systems and $1.93 million on-going beginning in FY 2024-25 in to maintain these critical state security systems.

Pros:

- Upgrades and maintains the State's IDS and IPS systems with contemporary security solutions.
- Consistent with the State's 2023 Vision Plan to protect the State's information assets, aligns with the Homeland Security Strategy, and eliminates individual state entity solutions.
- Maximizes state data access and improves the State's overall security maturity.

Cons:

- Increases General Fund spending.

ALTERNATIVE 2 – Utilize third party entities to upgrade and maintain the State's IDS and IPS security infrastructure and maintenance.

Pros:

- Upgrades and maintains the State's IDS and IPS systems with contemporary security solutions.
- Consistent with the State's 2023 Vision Plan to protect the State's information assets, aligns with the Homeland Security Strategy, and eliminates individual State entity solutions.

Cons:

- Utilizing 3rd party vendors would increase costs to the State regarding the development and ongoing maintenance of the IDS/IPS security solution
- Would take much longer for 3rd party vendors to deliver this security solution and would carry a higher degree of risk for successful implementation.
- This alternative would not be consistent with Government Code 19130 to utilize State employees.

ALTERNATIVE 3 – Do not approve this request and maintain the State's current IDS and IPS systems as they are.

Pros:

- No additional General Fund cost to the State.

Cons:

- Would leave the State increasingly vulnerable to a potential cybersecurity incident.
- Would not implement a contemporary defensively network perimeter that is necessary to meet industry standard security compliance requirements.
- Would not be consistent or comply with the State's 2023 Vision Plan to protect the State's information assets.
- The current obsolete IDS/IPS systems would leave the State increasingly vulnerable to a potential cybersecurity incident if they are not upgraded.

G. Implementation Plan

Once approved, CDT will continue validating devices, replacing those devices which have reached end of life, and will work through the procurement processes for the purchase of both Hardware and Software, to continue the maintenance needed to successfully utilize these IDS/ IPS devices for many years to come.

H. Supplemental Information

N/A

I. Recommendation

Approve CDT's GF request for $2.96 million in FY 2023-24 to upgrade the State's IDS/IPS systems and $1.93 million on-going in FY 2024/25 in to upgrade/maintain these critical state security systems. The proposed contemporary system upgrades are necessary for the State to continue to provide a frontline defense against malicious actors.

BCP Fiscal Detail Sheet

BCP Title: Intrusion Detection & Prevention System **BR Name: 7502-009-BCP-2023-GB**

Budget Request Summary

	FY23					
	CY	**BY**	**BY+1**	**BY+2**	**BY+3**	**BY+4**
Operating Expenses and Equipment						
5368 - Non-Capital Asset Purchases - Equipment	0	2,960	1,926	1,926	1,926	1,926
Total Operating Expenses and Equipment	**$0**	**$2,960**	**$1,926**	**$1,926**	**$1,926**	**$1,926**
Total Budget Request	**$0**	**$2,960**	**$1,926**	**$1,926**	**$1,926**	**$1,926**

Fund Summary

Fund Source - State Operations						
0001 - General Fund	0	2,960	1,926	1,926	1,926	1,926
Total State Operations Expenditures	**$0**	**$2,960**	**$1,926**	**$1,926**	**$1,926**	**$1,926**
Total All Funds	**$0**	**$2,960**	**$1,926**	**$1,926**	**$1,926**	**$1,926**

Program Summary

Program Funding						
6230 - Department of Technology	0	2,960	1,926	1,926	1,926	1,926
Total All Programs	**$0**	**$2,960**	**$1,926**	**$1,926**	**$1,926**	**$1,926**