STATE OF CALIFORNIA

Budget Change Proposal - Cover Sheet

DF-46 (REV 10/20)

Fiscal Year 2023-24	**Business Unit** 0555	**Department** California Environmental Protection Agency	**Priority No.**

Budget Request Name 0555-007-BCP-2023-GB	**Program** 0340-Support	**Subprogram**

Budget Request Description
Information Technology Security Posture

Budget Request Summary

The California Environmental Protection Agency (CalEPA) and its affiliated boards, departments, and offices (BDOs) are requesting $605,000 General Fund in 2023-24, and $555,000 General Fund in 2024-25 and ongoing to monitor and protect its information technology (IT) network, computer systems, and system components against cyberthreats and attacks on its IT assets. Cybersecurity monitoring is a detection strategy that uses tools and automation to continuously scan IT network systems for control weaknesses, suspicious activities, and alerting the CalEPA to mitigate information security risks before they lead to data breaches and resulting in public services disruption, data loss, financial losses, reputational damage, and/or loss of public trust.

Requires Legislation ☐ Yes ☒ No	**Code Section(s) to be Added/Amended/Repealed** None

Does this BCP contain information technology (IT) components? ☒ Yes ☐ No *If yes, departmental Chief Information Officer must sign.*	**Department CIO** Cruz Nieto, Acting AIO	**Date** 12/20/2022

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. **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 Mike Marshall	**Date** 1/10/2023	**Reviewed By** Eric Jarvis	**Date** 1/10/2023
Department Director Click or tap here to enter text.	**Date** Click or tap to enter a date.	**Agency Secretary** Yana Garcia	**Date** 1/10/2023

Department of Finance Use Only

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

PPBA Christian Beltran	**Date submitted to the Legislature** 1/10/2023

A. Budget Request Summary

The California Environmental Protection Agency (CalEPA) and its affiliated boards, departments, and offices (BDOs) are requesting $605,000 General Fund in 2023-24, and $555,000 General Fund in 2024-25 and ongoing to monitor and protect its information technology (IT) network, computer systems, and system components against cyberthreats and attacks on its IT assets. Cybersecurity monitoring is a detection strategy that uses tools and automation to continuously scan IT network systems for control weaknesses, suspicious activities, and alerting the CalEPA to mitigate information security risks before they lead to data breaches and resulting in public services disruption, data loss, financial losses, reputational damage, and/or loss of public trust.

B. Background/History

CalEPA consists of the Office of the Secretary and six BDOs. CalEPA's Office of the Secretary is responsible for developing a program to ensure that its BDOs take "consistent, effective and coordinated enforcement and compliance actions to protect public health and the environment." (GC § 12812.2 (a)(1).) While it shares the responsibility for environmental enforcement and compliance with its federal, local and tribal partners, the public expects the state of California to take the lead in assuring that environmental laws are enforced.

Of the BDOs within CalEPA, five have inspection and enforcement authority while OEHHA performs scientific evaluations that inform and guide regulatory environmental actions. Collectively, the BDOs enforce environmental laws that regulate air pollution from mobile and stationary sources; water quality and drinking water; hazardous waste and other toxic substances; the registration, sale, and use of pesticides; and solid waste recycling and source reduction. Information or data gathered from BDO inspection and enforcement processes are stored within a multitude of IT systems that are considered state infrastructure and/or mission critical systems.

CalEPA's uses information and data within its infrastructure and/or mission critical systems to support emergency response and recovery responsibilities. If hackers breach its website or system, they may view, edit or delete files across public networks. Hackers may also change the codes on CalEPA's website to stop it from functioning and cause public service disruptions or distortion of vital information during a statewide emergency.

With the rise in cyber-crime and data breaches, the state through the California Department of Technology (CDT) has pushed forward stricter security compliance standards in areas such as:

- Security programs – processes to protect the confidentiality and integrity of sensitive information and systems.
- Monitoring and testing – detection controls to analyze the effectiveness of technology supporting policy and process control; this includes penetration testing and independent audits.
- Risk assessments – analyzing internal and external cybersecurity threats, gaps in security controls, and vulnerabilities.
- Workforce and personnel – training and technical certification.
- Incident response – processes for detecting, investigating, mitigating, and documenting security events that lead to incidents.
- Security safeguards – system controls that protect and defend sensitive information, networks, and applications.

Driven by the collective need to secure its IT infrastructure including hardware, software, and IT systems against external cyberattacks and internal threats, CalEPA is taking an enterprise approach to improving its IT security posture. CalEPA and the BDOs have been working to improve the overall defense strategy by sharing knowledge, tools, and solutions that help in countering malicious attempts to steal, expose, alter, disable or destroy information through unauthorized access to computer systems. CalEPA is standardizing and leveraging shared IT procurement activities to lessen the complications of acquiring and deploying too many different software applications across the network infrastructure, and to keep track when to renew licenses, upgrade software versions, or remove/uninstall dormant software.

Security controls and privacy risks are the most common problems and pursuant to Government Code Section, 11549.3 (d), the CDT's Information Security Program Audit (ISPA) team is charged with evaluating state entities for compliance with state security and privacy policies, by validating security systems, procedures and practices are in place and working as intended. The ISPA team performs audits to ensure state entities are in compliance with requirement outline in the:

- State Administrative Manual (Chapter 5300)
- State Information Management Manual
- National Institute of Standards and Technology (NIST) Special Publication 800-53

An information security audit is a type of compliance audit that identifies potential cyber security gaps. It also provides guidance on implementing security procedures and privacy controls.

In addition to the ISPA, Government Code Section 11549.3 requires the California Military Department (CMD) to perform an Independent Security Assessments (ISA), which is a technical analysis of identified controls designed to measure Cyber Security Maturity. This analysis includes host vulnerability assessments, firewall analysis, host hardening analysis, phishing susceptibility, network penetration testing, and snap-shot analysis of network traffic for signs of threat actor compromise. The goal of the CMD ISA is to provide a view of the current security posture, an objective review of existing plans, and a guide to strategic planning. It also helps to develop tactical and strategic directions to further mature and strengthen its security program and compliance efforts.

Today, technology enables a faster, wider, and more efficient means of communication and interaction within each department, across departments, and to external entities and the public. Email, text messaging, social media, and other platforms are essential resources for communication. State government operations and services are taken online and into the cloud where it has capacity to build increasingly large complex infrastructures that rely heavily on digital technologies to connect systems and organize the flow of data between and among them. However, the increased capacity and system interconnection present increased risks and cyberthreats to critical infrastructure, systems, assets, and government operations. Cybercrimes are rampant and negatively affect the lives of people every year.

In recent years, ransomware has been a serious threat to businesses, non-profits, and government organizations alike. Cybercriminals rely on existing data breaches and stolen usernames and passwords sold on the Dark Web marketplace to target individuals and businesses, banking on many users who are still using the same passwords across different platforms. Upon infection, this malware holds valuable files hostage by encrypting them until a certain ransom is paid in the form of bitcoins, transfers, or any other form of digital currency. Examples of ransomwares include:

- Crypto ransomware, which encrypts files on a system.
- Locker ransomware locks a device's screen until the money is paid.
- Wiper ransomware deletes files from a hard drive.

In an ongoing effort to address these risks and cyberthreats, the CDT and its Office of Information Security (OIS) published *Cal-Secure*[1], California Executive Branch's first five-year information security maturity roadmap based on the frameworks and practices in the cybersecurity industry.

Cal-Secure lays out a plan for state entities to improve cyber security programs and ensure that resources are used to deal with the most critical problems in the cybersecurity system and keep the state's services safe.

While the CDT continues to work on key initiatives for consolidation such as:

[1] October 2021 https://cdt.ca.gov/wp-content/uploads/2021/10/Cybersecurity_Strategy_Plan_FINAL.pdf

- Create tools for cybersecurity strategy and roadmap development at state agencies and entities
- Formalize the cybersecurity governance structure
- Transform state information, privacy, and cybersecurity policies and standards
- Modernize cybersecurity procurement
- Create multi-tiered cybersecurity governance bodies

CalEPA and BDOs are initiating organizational change readiness by assessing the technology needs and taking actions based on the assessments from the ISPA and ISA.

Resource History
(Dollars in thousands)

Program Budget	**PY – 4**	**PY – 3**	**PY – 2**	**PY-1**	**PY**	**CY**
Authorized Expenditures	--	--	--	--	$1,053	$1,700
Actual Expenditures	--	--	--	--	--	--
Revenues	--	--	--	--	--	--
Authorized Positions	4.0	4.0	4.0	4.0	4.0	6.0
Filled Positions	4.0	4.0	4.0	4.0	4.0	4.0
Vacancies	--	--	--	--	--	2.0

C. State Level Consideration

This proposal addresses the following objectives from the Cal-Secure, the state of California Executive Branch Multi-Year Information Security Maturity Roadmap 2021:

- Continuous Vulnerability Management
- Asset Management
- Security Continuous Monitoring 24x7
- Application Development Security
- Log Management
- Network Access Control

This multi-year cybersecurity road map is designed to address critical gaps in the state's information and cybersecurity programs while enabling the state to manage existing and future threats more effectively. It includes a prioritized list of baseline cybersecurity capabilities that state entities must achieve over the next five years, including an anti-phishing program, security and privacy awareness training, and software supply chain management.

In a recent information security assessment by the California Military Department, several findings and recommendations to strengthen CalEPA's security posture were provided to mitigate unnecessary risks. Unnecessary risks could result in a breach which may cause extended business operational interruptions and disrupt CalEPA's critical role in public health and safety especially during the summer months when California is fighting wildfires, drought, air quality monitoring, and other statewide crises.

Additionally, this proposal is consistent with the following:

- Executive Order B-34-15 directing all state departments and agencies to ensure compliance with information security and privacy policies, promote awareness of information security standards with their workforce, and assist the California Governor's Office of Emergency Services and the California Cybersecurity Integration Center in executing this order.
- California State Auditor's Report 2015-611 recommends that state entities work with CDT to reach full compliance with security standards.
- California State Auditor's Report 2021-602 recommends that state law be amended to require that all state entities adopt information security standards and provide a confidential, annual status update on its compliance.

D. Justification

CalEPA requests $605,000 General Fund in 2023-24, and $555,000 General Fund in 2024-25 and ongoing to address cyber threats and potential attacks on the information technology (IT) network, computer systems, and system components.

The collective CalEPA and its BDOs enforce environmental laws that regulate air pollution from mobile and stationary sources; water quality and drinking water; hazardous waste and other toxic substances; the registration, sale, and use of pesticides; and solid waste recycling and source reduction. Information or data gathered from BDO inspection and enforcement processes are stored within a multitude of IT systems that are considered state infrastructure and/or mission critical systems. During statewide emergencies, such as major wildfires, CalEPA and its departments assist local, state, and federal agencies in recovery efforts. The services provided include emergency air monitoring by the California Air Resources Board, identification and removal of hazardous materials by the Department of Toxic Substances Control, and debris and ash removal by CalRecycle. The State Water Resources Control Board monitors water quality and ensures debris removal activities include measures to contain debris on site and prevent ash and other materials from entering rivers, creeks and streams.

Information and data within infrastructure and/or mission critical systems are crucial during emergency response and recovery efforts and must be protected from being disrupted, stolen, or exploited by unauthorized users. CalEPA is seeking funds to renew, expand, and negotiate enterprise-wide licensing agreements for the following tools and services that are part of the overall defense against cyber-attacks, including the management and strategy of protecting software, hardware, networks, services, and information. This proposal includes:

1. Governance, Risk, and Compliance (GRC) – CalEPA is increasingly look for ways to improve the relationship between risk management investment and business outcomes. Striking a balance between taking risks and imposing controls requires risk management principles and insights into strategic decision making. It also means risk teams must develop digital capabilities to harness risk intelligence across the enterprise. Such a vision — supported by the right Integrated Risk Management program, processes, and technology — is adaptive and well-suited to address new risks from cyber incident disruption, new regulatory obligation, and is imperative to building trust.

   The GRC platform connects the business, security, and Information Technology within an integrated risk framework and on the same platform. With a GRC platform, CalEPA and its BDOs can:

   - Control risk exposure. Use continuous monitoring and real-time dashboards to get actionable information about high-risk areas, noncompliance, vendor status, and significant audit findings.
   - Improve risk-based decision making. Plan and make decisions more strategically with a single integrated risk management program. Simplify communication and use context to assess business impact and prioritize activities.

- ➢ Increase performance. Boost performance and productivity with consistent cross-functional automation. Reduce errors and give CalEPA and its BDO's more time to focus on higher-value tasks.

A dynamic GRC includes powerful capabilities that drive cross-functional communication and processes, including a single data model to eliminate silos, automated workflows to reduce bottlenecks, and knowledge management to manage policies in one location.

2. Privileged Access Management (PAM) – Privileged Access Management (PAM) is an information security (infosec) mechanism that safeguards identities with special access or capabilities beyond regular users.

   CalEPA treats privileged accounts with extra care because of the risk they pose to the technology environment. For example, should the credentials of an administrator or service account fall into the wrong hands, it could lead to the compromise of the CalEPA Shared environment and confidential data.

3. Static application security testing (SAST) – SAST takes place very early in the software development life cycle (SDLC) as it does not require a working application and can take place without code being executed. It helps developers identify vulnerabilities in the initial stages of development and quickly resolve issues without breaking builds or passing on vulnerabilities to the final release of the application.

4. Networks Access Control (NAC)– Enables continuous visibility throughout the enterprise network and controls access to said network. Will provide us live inventory regarding what hardware/software are on the network including: users, classification, applications, open ports, vulnerabilities, indicators of compromise, and others). This tool will interrogate all endpoints which attempt to connect to the network and assure that they're patched and not nefarious prior to allowing on CalEPA's corporate network.

Table1. Itemized Request

Description	**2023-24**	**2024-25**
1. Governance, Risk, Compliance (GRC)	$100,000	$105,000
Governance, Risk, Compliance (GRC) Services	50,000	40,000
2. Privileged Access Management (PAM)	45,000	47,500
Privileged Access Management (PAM) Services	15,000	-
3. Static Application Security Testing	95,000	99,500
4. Network Access Control (NAC) Software/Hardware	250,000	263,000
Network Access Control (NAC) Services	50,000	-
Total	**$605,000**	**$555,000**

The CalEPA and its BDOs have many disparate systems and a variety of technology tools and platform to maintain and support. These systems handle critical program processes and are hard to replace. While some IT systems aged, others are upgraded, and new ones are acquired. Given the needs for compliance and data protection within its systems, California has adopted the National Institute of Standards and Technology[2] (NIST) Cybersecurity Framework. The Framework encompasses industry IT standards and best practices to help organizations manage cybersecurity risks. This framework was released in 2014 and became Public Law No: 113-274 in the same year. The Framework helps organizations understand cybersecurity risks (threats, vulnerabilities and impacts), and provides guidance on how to reduce these risks and how to respond and recover from cybersecurity incidents. The following five components make up the Cybersecurity Framework:

[2] NIST Framework. https://www.nist.gov/cyberframework/online-learning/five-functions

1. Identify: Understand and manage cybersecurity risk to systems, people, assets, data, and capabilities. Recognize potential risks based on the data that is regularly handled.
2. Protect: Outline appropriate safeguards to ensure delivery of critical infrastructure services. Invest in the appropriate protective technologies and implement security procedures.
3. Detect: Define the appropriate activities to identify the occurrence of a cybersecurity event. Enable timely discovery of cybersecurity events. Continuously monitor for cyber threats and system vulnerabilities.
4. Respond: Develop appropriate activities to take action regarding a detected cybersecurity incident. Contain the impact of a potential cybersecurity incident.
5. Recover: Identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. Timely recovery to normal operations to reduce the impact from a cybersecurity incident.

CalEPA and its BDOs are taking a collective approach to improving IT security posture by implementing the NIST Cybersecurity Framework. It has been sharing knowledge, tools, and security solutions level to build the security baseline. This proposal is a continuation of standardizing and leveraging shared IT-procurement activities to lessen the complications of acquiring and deploying too many different software applications across its network infrastructure. With a common tool set, CalEPA is working to shape and improve its overall cyber defense strategy.

As recent as January 2022, the California State Auditor's Office reported eight findings at the conclusion of an audit on information security practices of state entities within the Executive Branch. According to Report #2021-602, State High-Risk Update—Information Security[3]:

> *"Information security incidents that compromised the integrity, confidentiality, or availability of information have affected numerous retailers, government agencies, and financial institutions in recent years. Some of these security breaches have resulted in the disclosure of confidential information or the shutdown of information systems and critical infrastructure. For example, in June 2020, individuals launched a ransomware attack that encrypted the data on a number of servers at the University of California, San Francisco (UCSF) School of Medicine. To recover the data, UCSF paid approximately $1.1 million to the individuals behind the attack. In another example, in March 2021, an employee at the State Controller's Office (SCO) clicked on a link in an email that appeared to come from a trusted outside entity and unknowingly provided a hacker with access to reports that may have included individuals' full names, addresses, Social Security numbers, and birth dates. The hacker then sent malicious emails to the employee's contacts."*

One of the key highlighted findings in the report was that "…many reporting entities' information security is below standards and has not improved over the last several years." The State Auditor recommended that the Legislature amend state law to:

> *"Require each nonreporting entity to adopt information security standards comparable to those required by CDT and to provide a confidential, annual status update on its compliance with its adopted information security standards to legislative leadership, including the president pro tempore of the California State Senate, the speaker of the California State Assembly, and minority leaders in both houses. It should also require each nonreporting entity to perform or obtain an audit of its information security no less frequently than every three years."*

CalEPA is ultimately responsible for its own and its affiliated BDO's information security measures and compliance. The CDT and Military Department had previously observed and provided reports on CalEPA's potential system weaknesses and/or information security program deficiencies that require attention. Given the increasing number of cyber threats and incidents occurring daily, it is

[3] State Auditor: State High-Risk Update—Information Security. 01/18/2022. https://www.auditor.ca.gov/reports/2021-602/index.html#:~:text=CDT's%20intention%20is%20to%20provide,audits%20it%20should%20have%20finished.

essential that CalEPA fix any deficiencies and strengthen its security posture to more effectively guard against ransomware, data breaches, and other types of unwanted events to IT systems.

E. Outcomes and Accountability

Whereas CDT performs audits on state entities for compliance to the state's information security and privacy policies, the California Military Department performs an independent security assessment to evaluate the actual implementation, configuration, and practices of information security program. CDT established the California Cybersecurity Maturity Metrics to combine the results of the compliance audit and the security assessment into a single score for each reporting entity summarizing that entity's information security development. CDT designed the maturity metrics to be repeatable and consistent so that it can gauge each entity's progress moving forward.

The outcome of this proposal will be strengthening the collective CalEPA's cybersecurity posture and increasing the maturity score. The maturity scale is 0 (low maturity) to 4 (high maturity) and CalEPA is subject to recurring audits and assessment that measure how secure CalEPA is.

F. Analysis of All Feasible Alternatives

Alternative 1: Approve the request for $605,000 General Fund in 2023-24, and $555,000 General Fund in 2024-25 and ongoing to enable CalEPA to have the baseline security tools and software to make its security program more effective and successful.

Pros: This proposal will provide automated tools that can often catch gaps that are not found by people who are working within the network on a daily basis. This proposal is the next step forward in improving information security tools that will help us:

- Gain visibility into the security status of IT assets, networks, services, and information.
- Build controls and measure to protect from cyber-attacks, detect, respond and recover from attacks.
- Use automation to contain the impact of security attacks if/when they occur.

The tools being requested will help the security team understand the status of cybersecurity risks and vulnerabilities in its organizations so that it can close security gaps in the network and systems. This alternative will also allow for collaboration amongst BDO's technical staff, negotiation of pricing, promote technology standardization and the core value of being One CalEPA.

Cons: Implementing new software alone will not completely secure the network infrastructure. CalEPA still must know how to configure and use it effectively. Configuration and installation of new tools and software can take from a few weeks up to a few years depending on the requirements and size of each BDO. Time will be needed for thorough requirements gathering and product research and evaluations. Because this is a shared IT procurement effort, the input and feedback from team members could delay software implementation as it affects six other boards, departments, and offices who may have slightly different needs and roles in using the different products.

Alternative 2: Approve $895,000 in funding to address the immediate risks and findings related to security audit, compliance deficiencies, security risks, incident remediation activities, and/or other gaps as reported on the Plan of Action and Milestones (POAM). The POAM is mandated per SAM Section 5305.1 and follows a reporting process to CDT for addressing information security program deficiencies. These deficiencies have been observed as either potential system weaknesses or information security program deficiencies that require the agency to take steps to address, including short and longer-term plans, to avoid heighten risks of business disruptions especially during the summer months when California is fighting wildfires, drought, worsening air quality, or other statewide crises.

Pros: This alternative provides the following supplemental tools that are appropriate for remediation and/or mitigation of unnecessary risks that could result in a breach.

While also provided by CDT, the tools in this proposal may reduce the need for time-consuming activities such as manual reporting, complex spreadsheets, and confusing back-and-forth email tags when monitoring and detecting network abnormalities. They also may help the agency determine appropriate response procedures if a computer on the network has been compromised -- by aggregating information to answer questions such as:

- What are the indications that an incident has occurred or is currently in progress?
- What immediate actions should be taken?
- What forensic evidence can be preserved?

With the right tools to address current security findings, CalEPA will be able to correct deficiencies that have been open for more than 1 year pending budget augmentation.

Cons: Like Alternative 1, implementing new software alone will not completely secure the network infrastructure. CalEPA still must know how to configure and use it effectively. Configuration and installation of new tools and software can take from a few weeks up to a few years depending on the requirements and size of each BDO. Time will be needed for thorough requirements gathering and product research and evaluations. Because this is a shared IT procurement effort, the input and feedback from team members could delay software implementation as it affects six other boards, departments, and offices who may have slightly different needs and roles in using the different products.

<u>Alternative 3:</u> Maintain status quo.

CalEPA and its BDOs currently report remediation plan details related to a security audit finding, compliance deficiency, security risk, incident remediation activity, or other gap on the POAM. Each item on the POAM has a risk rating based on Threat Likelihood and Event Impact ratings as described in NIST Special Publication 800-30, ranging from very low, low, moderate, high, or very high. This alternative forces us to reexamine the risk impact of each item on the POAM to determine whether a finding should be accepted as a risk exposure without further budgetary action.

Pros: Risk management focuses on the negative—threats and failures rather than opportunities and successes. This alternative forces us to reexamine the impact of each item on the POAM and decide whether those with low or very low ratings are acceptable risks. If they are acceptable, remediation may not be required.

Cons: Proper levels of IT security are not negotiable. If appropriate steps are not taken to ensure the security of the organizations IT systems, CalEPA and its BDOs are at greater risk. The potential consequences of an IT security breach can have severe negative outcomes such as a negative perception or reputation that is extremely difficult to come back from. Other issues that can arise from a negative image is that employees don’t take security seriously, and rules and compliance do not matter.

G. Implementation Plan

Upon approval of this proposal, the CalEPA will coordinate to implement the following 3-year plan:

Year	**Activity**	**Details**
2022/23	Planning	1. Request budget augmentation 2. Prepare scope and requirements 3. Prepare staffing plan
2023/24	Procurement & Implementation	4. Acquire tools and software 5. Refine requirements

		6. Configure and install
2024/25	Maintenance & Operations	7. Deploy tools 8. Training and maintenance

H. Supplemental Information

The cost estimates used for this is based on previous purchase orders and informational price quotes from the IT vendor community. Estimates associated with Budget Year +1assume that any one-time installation services cost falls off and a standard 5% annual increase for licensing renewals is added on.

I. Recommendation

Alternative 1 is recommended. With the increase in frequency and complexity of security incidents and cyberthreats, CalEPA and its BDOs cannot afford to be unprepared. This alternative will provide the tools and software necessary to defend against threats before a breach occurs. Failing to be ready to respond when required may damage the state's reputation and high costs for recovery.

Analysis of Problem

BCP Fiscal Detail Sheet

BCP Title: Information Technology Security Posture

BR Name: 0555-007-BCP-2023-GB

Budget Request Summary

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
5346 - Information Technology	0	605	555	555	555	555
Total Operating Expenses and Equipment	**$0**	**$605**	**$555**	**$555**	**$555**	**$555**

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**	**$605**	**$555**	**$555**	**$555**	**$555**

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	605	555	555	555	555
Total State Operations Expenditures	**$0**	**$605**	**$555**	**$555**	**$555**	**$555**
Total All Funds	**$0**	**$605**	**$555**	**$555**	**$555**	**$555**

Program Summary

Program Funding

Program Funding	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
0340 - Support	0	605	555	555	555	555
Total All Programs	**$0**	**$605**	**$555**	**$555**	**$555**	**$555**