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

Fiscal Year	Business Unit	Department	Priority No.
2022-23	7100	Employment Development Department	

Budget Request Name	Program	Subprogram
7100-014-BCP-2022-GB	5920	

Budget Request Description
Cybersecurity Resilience and Instrumentation

Budget Request Summary
The Employment Development Department (EDD) requests a budget augmentation of $10.2 million General Fund in 2022-23, and $6.1 million in 2023-24 and 2024-25, and 29 cybersecurity positions to assist with fraud mitigation and to improve cybersecurity and suspicious event monitoring, response, and resiliency. This proposal includes funding for cybersecurity, enhancements, suspicious activity monitoring tools, and staff training and is necessary to proactively address cybersecurity vulnerabilities, threats and security findings, implement technology to mitigate benefit fraud, meet the increasing need in cyber risk management, and strengthen the EDD cybersecurity posture.

Requires Legislation	Code Section(s) to be Added/Amended/Repealed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 Rita Gass	Date 12/3/2021

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
Geoff Garcia	12/3/2021	Andy Bassi	12/3/2021
Department Director	**Date**	**Agency Secretary**	**Date**
Rita Saenz	12/8/2021	Natalie Palugyai	12/17/2021

Department of Finance Use Only

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

PPBA	Date submitted to the Legislature
Danielle Brandon	1/10/2022

A. Budget Request Summary

The Employment Development Department (EDD) requests a budget augmentation of $10.2 million General Fund in 2022-23and $6.1 million General Fund in 2023-24 and 2024-25, and 29 cybersecurity positions to assist with fraud mitigation and to improve cybersecurity and suspicious event monitoring, response, and resiliency. This proposal includes funding for cybersecurity, enhancements, suspicious activity monitoring tools, and staff training and is necessary to proactively address cybersecurity vulnerabilities, threats and security findings, implement technology to mitigate benefit fraud, meet the increasing need in cyber risk management, and strengthen the EDD cybersecurity posture.

B. Background/History

EDD is one of the largest state departments with employees at service locations throughout the state offering a wide variety of services to millions of Californians through Job Service, Unemployment Insurance (UI), Paid Family Leave (PFL), State Disability Insurance (SDI), Workforce Investment, and Labor Market Information programs. EDD's benefit programs administer billions of dollars in benefits each year to provide financial stability to workers and communities. As California's largest tax collection agency, EDD also handles the audit and collection of payroll taxes (over $80 billion in 2020-21) and maintains employment records for more than 18 million California workers.

The cyber threat landscape faced by EDD has been proven to be unprecedented and is global in nature, is very complex, and is the new normal. The EDD must consistently bolster its information security resources for protecting claimants, employers, and internal information.

California regulations and statutes place the responsibility on state agencies and departments, specifically to maintain its technology ecosystem while protecting the information contained therein. With the demand of customer needs for online services and making systems available 24 x 7 as well as the need to work remotely and recommendations from the Strike Team and CSA for implementing digital technologies, the EDD expanded its reliance on IT and automation. In addition to the cybersecurity risk that must be managed, the EDD experienced an unprecedented scale of cyber-attacks and fraud against the EDD systems. EDD is continuing to defend and protect against a worldwide effort to use Botnet (compromised computers that are controlled by cyber criminals) to deny EDD services to legitimate benefit claimants. These cyber-attacks and UI fraud tactics represent billions of dollars in fraudulent claims being paid out. Although, pandemic related benefit claims may decrease, cyber-attacks and benefit program fraud will still be there and the complexity will remain the same, if not, would become more complex.

In addition, EDD is continuously audited by control agencies such as Department of Labor (DOL), Internal Revenue Services (IRS), CA State Auditors, CA Department of Military, CA Department of Technology (CDT), and other internal/external required audits. Prior to the COVID-19 pandemic, the EDD had audit findings that dated as far back to 2016 that were not remediated. Most recently, EDD has accrued over 40 additional findings including business operational issues as a result of an independent security assessment and audit in 2020. The inability to address audit findings timely is due to the lack of resources, ineffectiveness of the current ITB structure of siloed security lines of business and lack of appropriate tools.

The EDD needs information security resources. The approval of the request for the additional positions and funding of security controls will increase EDD's ability to protect itself from compromise, proactively mitigate vulnerabilities, respond effectively and timely to any breach and proactively monitor and address the constant evolving cyber-attacks and benefit fraud tactics that are being utilized by individuals, organized criminals, and foreign nation state.

C. State Level Consideration

This proposal supports the Administration's strategic goal of sustainable and secure business operations by addressing the immediate cybersecurity and fraud challenges EDD faces. This will also build long-term, sustainable, and flexible processes that will allow EDD to serve the people of California securely. This proposal will ensure that EDD addresses issues raised by the California State Auditor, Strike Team, California Cybersecurity Integration Center (Cal-CSIC) and the Legislature regarding cybersecurity.

The state's UI program has drawn significant attention due to the substantial service challenges faced during the pandemic. The ITB is responsible for securing EDD's information systems and safeguarding information assets. Increasing ITB's capabilities and capacity is necessary in order for EDD to be successful. With the continued underfunding from the federal government, the department has no other options for additional funding to address these mission critical responsibilities.

This proposal directly addresses compliance with the following statewide directives, federal laws, and guidelines to safeguard the EDD's information, data, and technology:

- Executive Order B-34-15 – Increase California's preparedness to respond to cyber-attacks.
- Chapter 518, Statutes of 2015 (AB 670) – IT Security Assessments.
- Chapter 508, Statutes of 2016 (AB 1841) – Cyber-security Incident Response Planning.
- California Department of Technology Strategic Plan – Vision 2023.
- 20 CFR §603.9(b) (1): Requires unauthorized access and disclosure of Unemployment Compensation (UC) data.
- IRC §6103(p) (4): Requires that agencies receiving federal tax information (FTI) comply with Publication 1075 - Tax Information Security Guidelines for Federal, State and Local Agencies.
- Civil Code §1798.24(e): Requires agencies to keep an accounting of disclosures of personal information.
- SAM §5330: Requires each state entity to ensure compliance with information security requirements, both internally and externally.
- SAM §5335: Requires each state entity to continuously monitor its information systems for signs of suspicious or inappropriate activity.
- SAM §5335.1: Requires each state entity to implement a continuous monitoring program to facilitate ongoing awareness of vulnerabilities and to support risk management decisions.
- SIMM 5300-B: Foundational framework comprised of 30 priority security objectives to assist state entities with prioritization of their information security efforts.

D. Justification

This proposal is to fund a Cyber Security Division (CSD), augment staff focused on cybersecurity, supporting fraud related technologies risk management, and implement additional security and internal controls and tools, thus formalizing EDD's cybersecurity management program, mitigating security findings, enhancing and/or replacing inadequate security tools/solutions, procuring additional security control services essential in improving fraud mitigation practices and securing data entrusted to the EDD. Specifically, the requested additional IT resources, funding for cybersecurity technology tools and training will address the following:

- Continuous identification and mitigation of evolving cyber threats and fraud.
- Safeguard the security and integrity of the claimants and employers' data and other EDD information asset.
- Address the Plan of Action and Milestone audit and assessment findings by control agencies.
- Unify EDD's security lines of business into one division to streamline processes and effectively support EDD's mission in order to improve accountability and response management.
- Meet current and future workload demands due to ever increasing cyber threats and benefit fraud.
- Compliance with State and Federal policies.
- Implement security controls to support technical modernization against identity theft, identity fraud, ransomware, and cyber-attacks threats and reducing the risk and adverse impacts of data breaches.

Without the staffing increase and ability to modernize its security instrumentation and tools, the EDD will be constrained in its ability to secure, monitor, and respond to advancing security threats. This would place California's most critical benefit and tax programs at risk of compromise. Since the EDD's programs are needed the most during extreme economic downturns, the inability of EDD to protect these programs would have catastrophic impacts to California's most at-risk citizens.

Establish A Formal Cyber Security Program. Currently the EDD cybersecurity is managed via cross divisional lines within EDD ITB and a siloed Information Security Office. In addition, the current ITB resources are insufficient to adequately perform some of the functions essential to establish and sustain the EDD cybersecurity program as noted in the security findings conducted by the Department of Military and the Department of Technology. By establishing an adequately staffed CSD and consolidating the Information Security Office with all the security related functions across the Divisions, the EDD will have a robust and effective cybersecurity, and risk management program. This will allow the CSD to provide continuous improvement of the EDD cybersecurity program, deliver dedicated protection of critical UI, DI, Tax and Workforce systems and satisfy Information Security requirements as required by control agencies.

The justification substantiates the new Division structure and the request for the 29 new CSD permanent positions which includes a new Career Executive Assignment (CEA) level which will give cybersecurity more visibility, and much needed governance and authority that is lacking in the existing EDD structure. The new positions will be needed to resolve the audit findings, which are additional and unplanned workload that require analysis, evaluation of the findings, classification of the threat analysis and remediation as necessary while supporting the current and future workload.

The following is the breakdown of the requested positions:

- 1.0 CEA
- 1.0 IT Manager II
- 6.0 IT Manager I
- 1.0 IT Specialist III
- 11.0 IT Specialist II
- 8.0 IT Specialist I (Range C)
- 1.0 Office Technician (Typing)

The total cost of the staffing including salaries and benefits totals to $6.1 million annually.

Analysis of Problem

Integrated Risk Management (IRM)/Governance Risk and Compliance (GRC) Security Tool. The IRM and GRC security is necessary to support the EDD cybersecurity Program. The IRM and GRC tools included in this proposal total to $1.2 million. Along with the additional staffing, this tool will address the deficiencies of EDD's security governance and management cited by the CMD and CDT audits respectively. These tools will provide the following:

- Track cyber threat and fraud issues from identification through resolution.
- Comprehensive risk management framework (RMF) that includes risk appetite, risk calculation methodologies, risk acceptance criteria, risk categories, etc.
- Risk assessment methodology, detailed workflows, and procedures to identity, analyze, evaluate and treat information security risks.
- Policy and Compliance Management to develop a strong IT security risk program to meet current and future IT security assessments and CDT audit requirements.
- Risk management, real-time risk identification, business and IT service performance data, and requirement repository for automated controls testing, and continuous monitoring of the enterprise, and establishes a risk register and treatment plan.
- Ability to address and complete all identified IT security assessments and audit findings in a timely manner.
- Risk communication tools for inclusion of the business and Executive Management.
- Audit management for scoping and prioritization of audit engagements, enhancing audit assurance, and optimizing resources for internal audits.

Data Discovery and Classification Tool. This tool will allow EDD to be in accordance with SAM and SIMM policies of classifying all information assets (records, file, and /or databases). Each of these information assets requires categorization and classification for proper security controls to prevent unauthorized access or misuse. With automated tools to assist in the classification of information systems and information assets the risk of not having the appropriate safeguards in place to protect the information will be mitigated. With the automated tool and integration service(s) to implement an enterprise-wide data discovery and classification program, EDD will be able to automatically classify and categorize information, automate remediation of data and applicable security permissions, and automatically prohibit data from being stored or processed on inappropriate assets. The Data Discovery and Classification tool included in this proposal totals to $1.4 million. Implementing a Data Discovery and Classification tool will achieve the following:

- Create user awareness on data classifications and the appropriate handling of the data.
- Accurate data discovery, classification, and categorization of all data with minimal impact to EDD personnel.
- Automatically classify data within metadata and alternate data streams allowing other tools that EDD operates like, Data Loss Prevention systems, to ensure data moving from system to system or cloud services have correct classification and the ability to ensure only appropriate and authorized data is allowed in these systems.
- Persistent classification that cannot be changed by unauthorized users.
- Minimize data access to protect EDD data by ensuring appropriate security policies are enforced and identify when data was last accessed for record management and ensuring data is properly managed through its lifecycle.
- Assign accountability to data owners that will allow them to make appropriate decisions on how data is used internally and externally.

- Identify unsafe sensitive data and ensures remediation.
- Enforce data governance and streamline data discovery and classification processes.
- Comply with SAM, SIMM, IRS PUB 1075, and FIPS 199.

Application Security Assessment Tools. State agencies are mandated by SAM 5315.4 to develop and implement a system security test and evaluation plan. The EDD is further mandated by the IRS PUBLICATION 1075 to perform monthly vulnerability assessments of EDD's applications due to their interaction with Federal Taxpayer Information (FTI). EDD has numerous custom developed applications that leverage multiple programming languages, third-party open source plug-ins, Application Programming Interfaces (APIs), and public coding repositories to speed application delivery and improve the user experience. These applications serve the breadth of EDD's programs including Workforce Services, UI, SDI, PFL, and Employer Tax.

EDD does not currently possess the tools and resources to perform comprehensive security reviews of application code including third party libraries and publicly sourced code to identify and remediate potential exploitation points and system vulnerabilities. Software vulnerabilities are identified daily, and exploitation of those vulnerabilities are rapidly used by cyber criminals. EDD often relies on vendors to perform these security reviews prior to software releases. This dependency on external vendors would be reduced by developing this capability internally to EDD.

The EDD's applications have millions of lines of code that further complicate security reviews and remediation efforts. With EDD's rapid pace of system enhancement delivery, the EDD is not equipped to adequately ensure each optimization effort is thoroughly reviewed for new vulnerabilities.

The Application Security Assessment tools included in this proposal total to $1.5 million. For the EDD to meet its mandates and protect the integrity of EDD data, the Department requires modern security testing tools. These tools will provide the static and dynamic application security testing tools and software composition analysis to identify security vulnerabilities in integrated open-source and third-party application components, which will provide the following:

- Compliance with SAM and IRS PUBLICATION 1075, specifically where FTI is present.
- Capability to conduct thorough testing at the source code level.
- Complex coding will be reviewed and rapidly remediated, reducing the amount of time and effort for recoding, especially prior to code being used in production.
- All system enhancement efforts will be thoroughly tested prior to being placed into production for use by the claimants / customers of California.
- Ability for code to be secured across multiple user platforms like desktop web, mobile apps, and APIs.

- Ensures third party and open source libraries used with EDD coding are not vulnerable and understand what the current risks are by using them within EDD's code base.
- Updated tools ensure the EDD can defend against the newest, known vulnerabilities.

E. Outcomes and Accountability

This proposal supports the Administration's strategic goal of sustainable and secure business operations by addressing the immediate cybersecurity and benefit fraud challenges EDD faces while also building long-term, sustainable, and flexible processes that will allow EDD to better serve the people of California securely. This proposal will ensure that EDD addresses issues raised by the California State Auditor, Strike Team, Cal-CSIC, and the Legislature regarding security and benefit fraud.

The state's UI program has drawn significant attention due to the substantial service challenges faced during the pandemic. The ITB as a support Branch for the EDD's programs needs to be able to increase its capabilities and capacity in order for EDD to be successful. With the continued underfunding from the federal government, the department has no other options for additional funding.

Approving and funding the request for 29.0 positions, tools, training, and services and ongoing operating expenses will:

- Improve the EDDs cybersecurity posture, compliance with SAM, SIMM, IRS PUB 1075 regulations and the NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations.
- Provide CFSD with the capability to manage critical risks and findings identified in the CMD independent security assessment, and CDT audit.
- Reduce the risk of a data breach of claimant records, tax records and other EDD information assets.
- Allows the EDD to continue teleworking status in a safe and secure manner.
- Creates dedicated information security team(s) to monitor, detect, and prevent cyber-attacks and the evolving threats.
- A dedicated Cybersecurity team that will work with EDD program/business fraud specialist, to ensure technology is implemented and supported to enable fraud to be detected, prevented, and possibly recaptured.
- Protect confidential data of all Californians of working age from unlawful disclosure.
- Keep up with the higher demands from claimants/customers, and other EDD business programs for critical services.
- Provides the ability for the EDD to securely transition into a Cloud environment with sufficient tools, training, and staffing.
- Development of the CSD and workforce growth will provide better support and services to the EDDs business/benefit programs workforce growth.
- Improve facilitation and coordination of EDD data sharing between external public and private partners.
- Reduce the risk of litigation from data breaches.
- Provide the appropriate classifications and staffing levels with the correct tools, training and implementation services needed to support the EDD's mission, growth, compliance with State/federal rules and to prepare/respond to the evolving threat landscape.

F. Analysis of All Feasible Alternatives

Alternative 1: Approve funding request of $10.2 million in 2022-23, $6.1 million in 2023-24, and 29.0 ongoing positions to equip the EDD with advanced cybersecurity instrumentation through the following security tools: integrated risk management, data discovery and classification, and application security assessment, in addition to professional services to improve the EDD's cybersecurity monitoring, response, and resiliency.

Pros:

- Enhances the EDDs cyber security posture to allow the EDD to stop evolving threats, identify breaches faster, rapidly contain and remediate breaches, and reduce the resulting impact from breach occurrences.
- The EDD will improve its custom enterprise applications and infrastructure resiliency to compromise, through comprehensive training and improved staff skillsets.
- The EDD will be able to address security assessment and audit findings from the IRS, DOL, CSA, Cal-CSIC, CDT and CMD.
- Provides the necessary tools and implementation services to comply with State and Federal governance, risk, data classification and categorization policies and requirements.
- Ensures compliance with State and federal laws.
- Perform incident triage prioritization and response to notable events, which provides the best chance to stop cyber and other risks that threaten the ability to effectively deliver services in real time.
- Provide the means for improving monitoring, patching, hardening, perimeter security, access controls, account management, data classification, configuration management, IT asset management, IT application security, audit trails, phishing prevention, and risk assessment and management.

Cons:

- Requires an increase to EDD's appropriation that will impact the General Fund.

Alternative 2: Approve $6.1 million and 29.0 positions in 2022-23 to address cybersecurity workload.

Pros:

- EDD will have the necessary state staffing to begin enhancing the Department's cybersecurity posture.

Cons:

- Requires an increase to EDD's appropriation that will impact the General Fund.
- Without the security tools, the Department will not be able to improve its custom enterprise application's resiliency to compromise which may result in data breaches and reputational degradation.
- Without the security tools, the EDD will not be able to keep up with the rapidly evolving threat landscape impacting technology and government.
- IT staff without the required security tools will continue to rely on outdated knowledge and practices in the performance of their duties.
- Without the security tools, additional time will be spent trying to understand and address application issues which may expose EDD systems, and networks to cyber-attacks.

- Will not adequately address current and future security audit and assessment findings.
- Will not adequately reduce EDD's susceptibility to security breaches.
- May result in greater costs in the long-term, if systems are not monitored 24/7, coded correctly, or misconfigured due to lack of tools, implementation services, and training, due to potential compromised claimants/customer information, lost benefits, litigation costs, reputational damage and continued non-compliance with State and federal laws.

Alternative 3: Reject this BCP.

Pros:

- Does not require a General Fund augmentation.

Cons:

- Cyber threats will continue to be burdensome and a financial issue to the State, the EDD and claimants/customers data may be subject to ransomware or other types of attacks.
- The EDD will not be staffed or equipped with a modern toolset to assist the Department with proactively addressing security audit findings from the IRS, DOL, CSA, Cal-CSIC, CDT and CMD.
- The EDD will be at significant risk of not being able to meet the security assessment and audit finding remediation requirements for existing and future assessments and findings.
- The EDD will remain out of compliance with State and Federal policies and regulations which could jeopardize funding sources to the EDD.
- Exploitation points and system vulnerabilities will continue to go unchecked and non-remediated, putting all information assets at risk of data breach, exposing Personally Identifiable Information of all working Californians.
- Jeopardizes the short and long-term security and integrity of services provided by the EDD to claimants/customers.
- Jeopardizes the well-being of the claimant/customer if a cyber event cuts off their needed access to EDD funds because of lack of capability.
- The EDD information assets are at risk of misclassification, improper control safeguards, unauthorized access, and potential disclosure.
- Outdated tools and untrained IT staff will result in an ill-equipped IT branch and deficiencies in security preparedness, response and resilience.
- No cost in short term but will result greater costs in the long term, without the requested tools, training, implementation services, 24/7 monitoring and staffing needs, which could result in breached claimants/customer information, lost benefits, litigation costs, reputational damage, public distrust and continued non-compliance with State and federal laws.

G. Implementation Plan

The ITB will follow the below implementation plan. Part 1 and 2 of the plan are complete.

- Part 1: Design
  - IT Organizational Architecture: The ITB defined organizational design objectives, developed a strategically aligned capability map, and built a future IT operating model.

  - Organizational Sketch: The ITB assigned workload to units (accountabilities and responsibilities), defined roles by work units, turned roles into jobs, defined reporting relationships between jobs, assessed options and selected a go-forward organizational structure.

- Part 2: Structure
  - Organizational Structure: The ITB validated the organizational sketch, analyzed workforce utilization, defined competency framework, and identified competencies required for jobs.
  - Organizational Charts: The ITB determined the number of positions per job, conducted a competency assessment, assigned staff to jobs, and built a workforce and staffing plan.
- Part 3: Implement
  - Transition Strategy: The ITB will form an implementation team in partnership with the Human Resource Services Division (HRSD) to develop an organizational transition plan. The plan will include:
    - Establishing new and updating existing CEA policy concepts.
    - Finalizing the proposed organizational charts.
    - Creating and/or updating duty statements.
    - Preparing personnel packages to request to reorganize the current divisions as well as establish and recruit for new positions.
    - Obtaining HRSD and CalHR approval for the new and updated CEA. positions and overall reorganization.

Implement Structure: Upon approval of this proposal and the passage of the 2022-23 budget, the ITB will submit the reorganization request and corresponding personnel packages to HRSD. Once approved by HRSD and CalHR, the ITB will finalize the reorganization and begin the recruitment process for the new positions. Additionally, the ITB will train managers to lead through change, define and implement a stakeholder engagement plan, and develop and implement individual transition plans to help staff adapt to change and ensure a smooth reorganization process.

H. Recommendation

EDD recommends approving Alternative 1 as it will reduce the risk and adverse impacts of security attacks, data breaches, and will allow EDD to meet current and future workload demands. The creation of the CSD led by a new CEA, will enhance IT security across the EDD enterprise. EDD will be compliant with State and federal policies.

BCP Fiscal Detail Sheet

BCP Title: Cyber Security Resilience and Instrumentation

BR Name: 7100-014-BCP-2022-GB

Budget Request Summary

Personal Services

Personal Services	FY22 Current Year	FY22 Budget Year	FY22 BY+1	FY22 BY+2	FY22 BY+3	FY22 BY+4
Positions - Permanent	0.0	29.0	29.0	29.0	0.0	0.0
Total Positions	**0.0**	**29.0**	**29.0**	**29.0**	**0.0**	**0.0**
Salaries and Wages Earnings - Permanent	0	3,142	3,142	3,142	0	0
Total Salaries and Wages	**$0**	**$3,142**	**$3,142**	**$3,142**	**$0**	**$0**
Total Staff Benefits	0	1,941	1,941	1,941	0	0
Total Personal Services	**$0**	**$5,083**	**$5,083**	**$5,083**	**$0**	**$0**

Operating Expenses and Equipment

Operating Expenses and Equipment	FY22 Current Year	FY22 Budget Year	FY22 BY+1	FY22 BY+2	FY22 BY+3	FY22 BY+4
5301 - General Expense	0	62	62	62	0	0
5304 - Communications	0	39	39	39	0	0
5322 - Training	0	101	101	101	0	0
5324 - Facilities Operation	0	186	186	186	0	0
5326 - Utilities	0	11	11	11	0	0
5340 - Consulting and Professional Services - External	0	1,200	0	0	0	0
5344 - Consolidated Data Centers	0	62	62	62	0	0
5346 - Information Technology	0	71	71	71	0	0
539X - Other	0	3,343	468	468	0	0
Total Operating Expenses and Equipment	**$0**	**$5,075**	**$1,000**	**$1,000**	**$0**	**$0**

Total Budget Request

Total Budget Request	FY22 Current Year	FY22 Budget Year	FY22 BY+1	FY22 BY+2	FY22 BY+3	FY22 BY+4
Total Budget Request	**$0**	**$10,158**	**$6,083**	**$6,083**	**$0**	**$0**

Fund Summary

Fund Source

Fund Source	FY22 Current Year	FY22 Budget Year	FY22 BY+1	FY22 BY+2	FY22 BY+3	FY22 BY+4
State Operations - 0001 - General Fund	0	10,158	6,083	6,083	0	0
Total State Operations Expenditures	**$0**	**$10,158**	**$6,083**	**$6,083**	**$0**	**$0**
Total All Funds	**$0**	**$10,158**	**$6,083**	**$6,083**	**$0**	**$0**

Program Summary

Program Funding

Program Funding	FY22 Current Year	FY22 Budget Year	FY22 BY+1	FY22 BY+2	FY22 BY+3	FY22 BY+4
5920 - Unemployment Insurance Program	0	10,158	6,083	6,083	0	0
Total All Programs	**$0**	**$10,158**	**$6,083**	**$6,083**	**$0**	**$0**

Personal Services Details

Positions

Positions	FY22 Current Year	FY22 Budget Year	FY22 BY+1	FY22 BY+2	FY22 BY+3	FY22 BY+4
1139 - Office Techn (Typing)	0.0	1.0	1.0	1.0	0.0	0.0
1401 - Info Tech Assoc	0.0	8.0	8.0	8.0	0.0	0.0
1405 - Info Tech Mgr I	0.0	6.0	6.0	6.0	0.0	0.0
1406 - Info Tech Mgr II	0.0	1.0	1.0	1.0	0.0	0.0
1414 - Info Tech Spec II	0.0	11.0	11.0	11.0	0.0	0.0
1415 - Info Tech Spec III	0.0	1.0	1.0	1.0	0.0	0.0
7500 - - C.E.A. - A	0.0	1.0	1.0	1.0	0.0	0.0
Total Positions	**0.0**	**29.0**	**29.0**	**29.0**	**0.0**	**0.0**

Salaries and Wages

Salaries and Wages	FY22 Current Year	FY22 Budget Year	FY22 BY+1	FY22 BY+2	FY22 BY+3	FY22 BY+4
1139 - Office Techn (Typing)	0	44	44	44	0	0
1401 - Info Tech Assoc	0	789	789	789	0	0
1405 - Info Tech Mgr I	0	706	706	706	0	0
1406 - Info Tech Mgr II	0	135	135	135	0	0
1414 - Info Tech Spec II	0	1,189	1,189	1,189	0	0
1415 - Info Tech Spec III	0	119	119	119	0	0
7500 - - C.E.A. - A	0	160	160	160	0	0
Total Salaries and Wages	**$0**	**$3,142**	**$3,142**	**$3,142**	**$0**	**$0**

Staff Benefits

Staff Benefits	FY22 Current Year	FY22 Budget Year	FY22 BY+1	FY22 BY+2	FY22 BY+3	FY22 BY+4
5150150 - Dental Insurance	0	24	24	24	0	0
5150200 - Disability Leave - Industrial	0	7	7	7	0	0
5150210 - Disability Leave - Nonindustrial	0	4	4	4	0	0
5150350 - Health Insurance	0	569	569	569	0	0
5150500 - OASDI	0	184	184	184	0	0
5150600 - Retirement - General	0	991	991	991	0	0
5150700 - Unemployment Insurance	0	3	3	3	0	0
5150750 - Vision Care	0	4	4	4	0	0

Staff Benefits	FY22 Current Year	FY22 Budget Year	FY22 BY+1	FY22 BY+2	FY22 BY+3	FY22 BY+4
5150800 - Workers' Compensation	0	107	107	107	0	0
5150900 - Staff Benefits - Other	0	48	48	48	0	0
Total Staff Benefits	**$0**	**$1,941**	**$1,941**	**$1,941**	**$0**	**$0**

Total Personal Services

Total Personal Services	FY22 Current Year	FY22 Budget Year	FY22 BY+1	FY22 BY+2	FY22 BY+3	FY22 BY+4
Total Personal Services	**$0**	**$5,083**	**$5,083**	**$5,083**	**$0**	**$0**