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

Fiscal Year	Business Unit	Department	Priority No.
2023-24	7100	Employment Development Department	

Budget Request Name	Program	Subprogram
7100-050-BCP-2023-MR	5920, 5925	

Budget Request Description
Cybersecurity Software Licensing

Budget Request Summary
The Employment Development Department (EDD) requests a budget augmentation of $3,346,000 for 2023-24 and ongoing, funded equally by the EDD Contingent Fund and the Unemployment Compensation Disability Fund, to continue licensing critical automated tools used by the Cybersecurity Division to scan, identify, and respond to vulnerabilities and threats; escalate and report security incidents and data breaches; and track and respond to federal and state mandated cybersecurity audits and compliance reports.

Requires Legislation	Code Section(s) to be Added/Amended/Repealed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 1/25/2023

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 García/Cathy Parr	1/25/2023	Jeff Loverde	1/25/2023
Department Director	**Date**	**Agency Secretary**	**Date**
Nancy Farias	2/3/2023	Stewart Knox	2/7/2023

Department of Finance Use Only

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

PPBA	Date submitted to the Legislature
Andrew March	3/30/2023

A. Budget Request Summary

The Employment Development Department (EDD) requests a budget augmentation of $3,346,000 for 2023-24 and ongoing, funded equally by the EDD Contingent Fund and the Unemployment Compensation Disability Fund, to continue licensing critical automated tools used by the Cybersecurity Division to scan, identify, and respond to vulnerabilities and threats; escalate and report security incidents and data breaches; and track and respond to federal and state mandated cybersecurity audits and compliance reports.

B. Background/History

The EDD is one of the largest state departments in California 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), 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, the EDD handles the audit and collection of payroll taxes (over $109.3 billion in 2021-22), processes employer documents and electronic payments (over 53.4 million documents in 2021-22) and maintains the wage records for more than 18.5 million California workers.

Expanded online services and the expectation of continuous systems availability has significantly increased both the public and the EDD's reliance on IT automation over the last few years. Due to the nature of the services offered and the data maintained within its systems, this has made the EDD a significant target for cybersecurity criminals. The department continues to experience an increase in cyber-attacks monthly. These attacks are both national and global in nature and use Botnet technology, defined as compromised computers that are controlled by cyber criminals, to deny services to legitimate benefit claimants. Additionally, cyber criminals continue to use phishing, and other means to attempt to gain access to EDD data resources. The EDD cybersecurity teams combat these attacks using combined automated threat and vulnerability assessment tools to constantly scan networks, applications and operating systems for threats and weaknesses. The teams also use these tools to proactively scan coding changes to systems and networks to ensure that changes are planned, built, tested, and released consistent with the Information Security Office (ISO) policies and standards and NIST 800-53 requirements.

The ISO is responsible for developing and maintaining cybersecurity policies and standards consistent with state and federal requirements across EDD. ISO staff perform security reviews on EDD systems, IT projects, and processes to ensure compliance to policy and standards. If the system, project, or process deviates from the ISO security standards, the project sponsor, system owner, or data owner must submit a Risk Acceptance Request through the EDD's integrated risk management application explaining the nature of the risk, steps taken to mitigate or correct the risk, and obtain approval from executive leadership. During the last two years, EDD has completed over 200 IT projects requiring security reviews. Any risk acceptance from those projects requires the risk to be reevaluated annually requiring ongoing tracking and reporting through the automated risk management system. Additionally, EDD is currently starting to develop key new technology solutions via the EDDNext project to replace legacy IT infrastructure and systems that will require security reviews and tracking of risk items.

The ISO also reviews firewall change requests and other enterprise and architecture change requests that must be submitted as service tickets to ensure any additions or changes in firewall

infrastructure meet ISO standards. In the last six years, the ISO has received 1,465 firewall change requests averaging 244 requests a year, or 20 each month.

In 2022-23, the EDD was authorized 29.0 new positions to bolster the Information Security Office to create the Cybersecurity Division (CSD) and expand the department's ability to perform task and activities associated with the various cybersecurity functions. The EDD worked with the California Department of Human Resources to align existing Information Security Office positions with the new positions. The CSD is comprised of five cybersecurity units responsible for unique aspects of cybersecurity management activities. This process took approximately five months to complete and the CSD became operational on January 1, 2023. As of this date, three managers have been hired and have begun the work of recruiting and training staff.

In addition to the expansion of cybersecurity staff, the EDD was authorized one-time funding for the purchase of the cybersecurity software and tools necessary to perform daily scanning, monitoring, assessment, reporting, resolution and auditing tasks and activities within the new CSD.

Since July 2022, the ISO (CSD as of January 2023) is actively procuring all the cybersecurity tools defined in the 2022-23 Budget Change Proposal (BCP). The tools to be procured include the combined Integrated Risk Management/Governance Risk and Compliance tool as part of an integrated Cybersecurity suite of tools, the Data Discovery and Classification tool, and the Application Security Code Assessment tool. The Application Security Code Assessment tool will begin production use in February 2023, focusing on critical applications supporting EDD's benefit programs. All the tools have been purchased through one-time funding through the 2022-23 BCP. The CSD is developing plans for the installation, configuration, policy development, training, and roll out for each tool.

C. State Level Consideration

This proposal will allow the EDD to continue effectively supporting the Administration's strategic goal of sustainable and secure business operations by addressing and responding to threats and fraud challenges. EDD will need to continue using the cybersecurity integrated risk management (IRM), data discovery and classification, and application security assessment tools. The EDD requires these tools to maintain 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) – Cybersecurity Incident Response Planning.
- California Department of Technology Strategic Plan – Vision 2023.
- Governor's Cal-Secure multi-year initiative.
- 20 Code of Federal Regulations section 603.9(b) (1): Requires unauthorized access and disclosure of Unemployment Compensation (UC) data.
- Internal Revenue Code section 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 section 1798.24(e): Requires agencies to keep an accounting of disclosures of personal information.
- State Administrative Manual (SAM) section 5330: Requires each state entity to ensure compliance with information security requirements, both internally and externally.
- SAM section 5335: Requires each state entity to continuously monitor its information systems for signs of suspicious or inappropriate activity.
- SAM section 5335.1: Requires each state entity to implement a continuous monitoring program to facilitate ongoing awareness of vulnerabilities and to support risk management decisions.
- Statewide Information Management Manual (SIMM) section 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 requests ongoing funding for the renewal of cybersecurity software and tools that are essential in fraud mitigation practices and for securing data entrusted to the EDD. Without the continued deployment of its security instrumentation, the EDD will be constrained in its ability to secure, monitor, and respond to advancing security threats. This would place California's critical benefits 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 at-risk citizens which includes, but not limited to the following:

- Loss of continuous identification and mitigation of evolving cyber threats and fraud.
- Loss of safeguarding the security and integrity of the claimants and employers' data and other EDD information assets.
- An inability to effectively address the multitude of Plan of Action and Milestone audits and assessment findings by various control and oversight agencies.
- An inability to meet current and future workload demands due to reduced response time due to lack of automation.
- Risk of non-compliance with State and Federal policies.
- Inability to identify and monitor security controls that support technical modernization against identity theft, identity fraud, ransomware, and cyber-attacks threats and reducing the risk and adverse impacts of data breaches.

The software listed below are tools currently used by CSD, which requires ongoing licensing to perform the Cyber security tasks performed by EDD:

1. **Cybersecurity Management Tool Suite**. This item was budgeted one-time in 2022-23 for $1,200,000 for an Integrated Risk Management tool suite. The ongoing renewal cost is $1,300,000 annually.

   The Cybersecurity Management Tool Suite includes the following four components:

   - **IRM/Governance Risk Management and Compliance (GRC) Security Tool.** The IRM and GRC security tool supports the EDD CSD Integrated Risk Program allowing the program to facilitate, record, track, and address control agencies audits from the Department of Labor (DOL), Internal Revenue Services (IRS), CA State Auditors (CSA), and CA Department of

Military (CDM), and the California Department of Technology (CDT). This constitutes a minimum of six recurring cybersecurity related audits yearly as well as ad hoc audits from a variety of entities that include cybersecurity components. In October 2020, the CDT began requiring the EDD to complete the annual California Compliance and Security Incident System (Cal-CSIRS) report on all mission critical systems. The report consists of more than 2,000 questions per report per system in accordance with the National Institute of Standards and Technology (NIST 800-53) standards for information security. This constitutes 50,000 security control questions answerable by the EDD CSD Security Risk & Integrated Risk Management team on an annual basis.

- **Incident Management & Request Tracking Tool**. Allows CSD to identify and respond to security incidents and requests for assistance in a timely and effective manner in alignment with NIST 800-53's requirements for incident response planning and procedures.
- **Electronic Catalog of EDD Assets.** Organizes and manages the request, approval, and delivery of security requests in alignment with NIST 800-53's requirement for service management controls. The catalog of assets is a required component of asset identification and incident reporting in compliance with State Administrative Manual (SAM) 5315.4 and IRS Publication 1075. Provides service request submission, service request tracking, and service request fulfillment processes.
- **Security Change Management Tool**. Provides threat and vulnerability assessment to ensure that changes to infrastructure, systems, applications, and networks are properly planned, tested, and implemented, in alignment with NIST 800-53's requirement for change management controls to minimize risk of security vulnerabilities introduced by changes in systems and networks.

2. **Data Discovery and Classification Tool.** This item was budgeted one-time in 2022-23 for $1,000,000 (Data Discovery and Classification) and the ongoing renewal cost is $1,185,000 annually. This tool monitors for threat and vulnerability within EDD systems and data storage devices. It allows the EDD to operate in accordance with SAM and SIMM policies for categorizing and classifying all information assets such as records, files, and databases to validate for proper security controls that will help prevent unauthorized access or misuse. The tool also tracks the classification of each information system and asset within EDD and categorizes the level of risk incurred for not having the appropriate safeguards in place to protect systems and assets. It then tracks the security controls in place around each asset to ensure the asset is appropriately monitored to enforce security control in the event of attempted improper usage. It also automatically prohibits data from being stored or processed on inappropriate assets.

The Data Discovery and Classification Tool maintains the following:

- Creates user awareness of data classifications and the expected handling of the data.
- Allows for the continued accurate data discovery, classification, and categorization of all data with minimal impact to EDD personnel.
- Automatically classifies data within metadata and alternate data streams allowing other tools operated within the EDD such as its data loss prevention systems to ensure data moving from system to system or into cloud services have correct classification and the ability to ensure only appropriate and authorized data is allowed in these systems.
- Provides persistent classification that cannot be changed by unauthorized users.
- Minimizes data access to protect EDD data by ensuring appropriate security policies are enforced and identified when data was last accessed for record management and ensuring data is properly managed through its lifecycle.
- Assigns accountability to data owners allowing them to make appropriate decisions on how data is used internally and externally.
- Identifies unsafe sensitive data and ensures remediation.
- Enforces data governance and streamline data discovery and classification processes.
- Compliance with SAM, SIMM, IRS Publication 1075, and Federal Information Processing Standards Publication 199.

3. **Application Security Source Code Assessment Tool**. This item was budgeted one-time in 2022-23 for $1,475,000 (Application Security Assessment) and the ongoing renewal cost is $861,000 annually.

   State agencies are mandated by SAM section 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 (API), 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.

   The Application Security Source Code Assessment Tool maintains the following:

   - Compliance with SAM and IRS Publication 1075, specifically where FTI is present.
   - Capability to conduct thorough testing at the source code level.
   - Ability to review and rapidly remediate complex coding, reducing the amount of time and effort for recoding, especially prior to code being used in production.

- Thoroughly test system enhancement efforts prior to being placed into production for use by the claimants and customers of California.
- Ability for code to be secured across multiple user platforms like desktop web, mobile apps, and APIs.
- Ensure third party and open-source libraries used with EDD coding are not vulnerable and provide an understanding of what the current risks are by using them within EDD's code base.
- Ensure that EDD can defend against the newest, known vulnerabilities.

Summary of Funding Request

Software Tools	**2023-24** (and Ongoing)
Cybersecurity Management Tool Suite	$1,300,000
Data Discovery and Classification Tool	$1,185,000
Application Security Source Code Assessment Tool	$861,000
Total	**$3,346,000**

E. Outcomes and Accountability

The proposal supports the Administration's strategic goal of sustainable and secure business operations by addressing the cybersecurity threats and fraud challenges that the EDD faces daily, while also building long-term, sustainable, secure, and flexible processes that allow the EDD to better serve the people of California. The procurement of cybersecurity tools will result in the following:

- Allow the EDD to maintain its security posture and compliance with SAM, SIMM, IRS PUB 1075 regulations and the NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations.
- Provide the EDD with the capability to manage critical risks and findings identified in the CMD independent security assessment, and the CDT audit.
- Reduce the risk of data breaches of claimant records, tax records and other EDD information assets.
- Allow dedicated information security teams to effectively monitor, detect, and prevent cyberattacks and evolving threats.
- Allow dedicated team liaisons within the EDD programs including business fraud specialists to continue scanning and monitoring their systems for fraud detection, prevention, and possible recapture.
- Protect confidential data of all Californians against unlawful disclosure.
- Prevent disruption of critical services due to malicious cybersecurity attacks.
- Support the EDD's ability to continue transitioning into a secure cloud-based environment.

- Continue to improve the facilitation and coordination of EDD data sharing between external public and private partners.
- Reduce the risk of litigation from data breaches.
- Facilitate CSD's mission, growth, compliance with state/federal rules.
- Prepare, respond, and report to the evolving threat landscape.

F. Analysis of All Feasible Alternatives

Failure to obtain funding for the ongoing licensing fees for the EDD's cybersecurity software and tools will put the EDD at significant risk of cybersecurity breaches and events. Additionally, without continued funding of these tools, EDD will be out of compliance with state and federal standards for cybersecurity and will continue to be out of compliance with audit findings from past CDT and CMD audits and assessments. There are no feasible alternatives to the use of these tools.

Alternative 1: Approve funding request of $3,346,000 in 2023-24 and ongoing to enable the EDD to continue using advanced cybersecurity instrumentation to improve the EDD's cybersecurity monitoring, response, and resiliency.

Pros:

- The EDD will continue to improve its cybersecurity posture and allow the EDD to stop evolving threats, identify breaches faster, rapidly contain and remediate breaches, and reduce the resulting impact from breach occurrences.
- Provide the necessary tools to comply with State and Federal governance, risk, data classification and categorization policies and requirements.
- 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 a budget augmentation in EDD's Contingent Fund and Disability Fund appropriation.

Alternative 2: Reject this proposal.

Pros:

- A budget augmentation will not be required.

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 equipped with a modern toolset to assist the Department with proactively addressing security audit findings from the IRS, DOL, CSA, Cal-CSIRS, 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.
- No cost in short term but will result greater costs in the long term, without the requested tools, 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

This BCP is seeking ongoing funding for the licensing of software and tools that are already rolled out or in the process of being rolled out within EDD. No further implementation will be required.

H. Supplemental Information

Attachment I – List of Information Technology items.

I. Recommendation

EDD recommends the approval of Alternative #1 to provide the requested ongoing funding for the continued licensing fees of the EDD's cybersecurity software and tools to safeguard EDD's systems and applications.

BCP Fiscal Detail Sheet

BCP Title: Cybersecurity Software Licensing

BR Name: 7100-050-BCP-2023-A1

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	3,346	3,346	3,346	3,346	3,346
Total Operating Expenses and Equipment	**$0**	**$3,346**	**$3,346**	**$3,346**	**$3,346**	**$3,346**

Total Budget Request

Total Budget Request	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
Total Budget Request	**$0**	**$3,346**	**$3,346**	**$3,346**	**$3,346**	**$3,346**

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 - 0185 - Employment Development Department Contingent Fund	0	1,673	1,673	1,673	1,673	1,673
State Operations - 0588 - Unemployment Compensation Disability Fund	0	1,673	1,673	1,673	1,673	1,673
Total State Operations Expenditures	**$0**	**$3,346**	**$3,346**	**$3,346**	**$3,346**	**$3,346**
Total All Funds	**$0**	**$3,346**	**$3,346**	**$3,346**	**$3,346**	**$3,346**

Program Summary

Program Funding

Program Funding	FY23 Current Year	FY23 Budget Year	FY23 BY+1	FY23 BY+2	FY23 BY+3	FY23 BY+4
5920 - Unemployment Insurance Program	0	1,673	1,673	1,673	1,673	1,673
5925 - Disability Insurance Program	0	1,673	1,673	1,673	1,673	1,673
Total All Programs	**$0**	**$3,346**	**$3,346**	**$3,346**	**$3,346**	**$3,346**

7100-050-BCP-2023-MR

	CY	BY	BY+1	BY+2	BY+3	BY+4
Positions						
Permanent	0.0	0.0	0.0	0.0	0.0	0.0
Temporary	0.0	0.0	0.0	0.0	0.0	0.0
Exempt	0.0	0.0	0.0	0.0	0.0	0.0
Board	0.0	0.0	0.0	0.0	0.0	0.0
Total Positions	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**
Salaries and Wages						
Earnings - Permanent	0	0	0	0	0	0
Earnings - Temporary	0	0	0	0	0	0
Earnings - Statutory/Exempt	0	0	0	0	0	0
Overtime, Holiday, Other	0	0	0	0	0	0
Total Salaries and Wages	**$0**	**$0**	**$0**	**$0**	**$0**	**$0**
Staff Benefits						
Dental Insurance	0	0	0	0	0	0
Disability Leave	0	0	0	0	0	0
Health Insurance	0	0	0	0	0	0
Life Insurance	0	0	0	0	0	0
Medicare Taxation	0	0	0	0	0	0
OASDI	0	0	0	0	0	0
Retirement	0	0	0	0	0	0
Unemployment Insurance	0	0	0	0	0	0
Vision Care	0	0	0	0	0	0
Workers' Compensation	0	0	0	0	0	0
Staff Benefits - Other	0	0	0	0	0	0
Total Staff Benefits	**0**	**0**	**0**	**0**	**0**	**0**
Total Personal Services	**$0**	**$0**	**$0**	**$0**	**$0**	**$0**
Operating Expenses and Equipment						
General Expense	0	0	0	0	0	0
Printing	0	0	0	0	0	0
Communications	0	0	0	0	0	0
Postage	0	0	0	0	0	0
Insurance	0	0	0	0	0	0
Travel	0	0	0	0	0	0
Training	0	0	0	0	0	0
Facilities Operations	0	0	0	0	0	0
Utilities	0	0	0	0	0	0
Consulting and Professional Services	0	0	0	0	0	0
Departmental Services	0	0	0	0	0	0
Consolidated Data Centers	0	0	0	0	0	0
Information Technology	0	3,346,000	3,346,000	3,346,000	3,346,000	3,346,000
Central Administrative Services	0	0	0	0	0	0
Office Equipment	0	0	0	0	0	0
Other	0	0	0	0	0	0
Unclassified/Special Adjustment	0	0	0	0	0	0
Total Operating Expenses and Equipment	**$0**	**$3,346,000**	**$3,346,000**	**$3,346,000**	**$3,346,000**	**$3,346,000**
Total Budget Request	**$0**	**$3,346,000**	**$3,346,000**	**$3,346,000**	**$3,346,000**	**$3,346,000**
Fund Source - State Operations						
General Fund	0	0	0	0	0	0
Federal Funds	0	0	0	0	0	0
Other/Special Funds	0	3,346,000	3,346,000	3,346,000	3,346,000	3,346,000
Reimbursements	0	0	0	0	0	0
Total State Operations Expenditures	**$0**	**$3,346,000**	**$3,346,000**	**$3,346,000**	**$3,346,000**	**$3,346,000**
Fund Source - Local Assistance						
General Fund	0	0	0	0	0	0
Federal Funds	0	0	0	0	0	0
Other/Special Funds	0	0	0	0	0	0
Reimbursements	0	0	0	0	0	0
Total Local Assistance Expenditures	**$0**	**$0**	**$0**	**$0**	**$0**	**$0**

Supplemental Information

(Dollars in thousands)

BCP No.	Proposal Title
7100-050-BCP-2023-MR	Cybersecurity Software Licensing and Tools

Information Technology	CY	BY	BY +1	BY +2	BY +3	BY +4
Cybersecurity Management Tool Suite		$ 1,400	$ 1,400	$ 1,400	$ 1,400	$ 1,400
Data Discovery and Classification Tool		$ 1,185	$ 1,185	$ 1,185	$ 1,185	$ 1,185
Application Security Source Code Assessment Tool		$ 861	$ 861	$ 861	$ 861	$ 861
Threat & Vulnerability Assessment & Monitoring Tools		$ 310	$ 310	$ 310	$ 310	$ 310
Total	$ -	**$ 3,756**	**$ 3,756**	**$ 3,756**	**$ 3,756**	**$ 3,756**