

STATE OF CALIFORNIA
Budget Change Proposal - Cover Sheet
 DF-46 (REV 08/15)

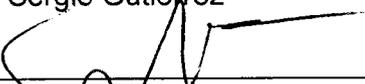
Vfd3

Fiscal Year 2016-17	Business Unit 0555	Department California Environmental Protection Agency	Priority No. 1
Budget Request Name 0555-001-BCP-BR-2016-GB		Program 0340-SUPPORT	Subprogram N/A

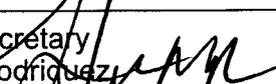
Budget Request Description
 California Environmental Protection Agency Cyber Security Workload Growth

Budget Request Summary

The California Environmental Protection Agency is requesting funding of \$1.1 million from multiple special fund sources and 4.0 permanent positions, to accommodate workload growth associated with increased demands for securing the California Environmental Protection Agency's critical Information Technology assets from compromise or business impact, and ensuring the confidentiality, integrity, and privacy of confidential information.

Requires Legislation <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	Code Section(s) to be Added/Amended/Repealed	
Does this BCP contain information technology (IT) components? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No <i>If yes, departmental Chief Information Officer must sign.</i>	Department CIO Sergio Gutierrez 	Date 1-6-16
For IT requests, specify the date a Special Project Report (SPR) or Feasibility Study Report (FSR) was approved by the Department of Technology, or previously by the Department of Finance. <input type="checkbox"/> FSR <input type="checkbox"/> SPR Project No. 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 Sergio Gutierrez	Date 1-6-16	Reviewed By Alice Stebbins, Division Chief 	Date
Department Director Eric Jarvis, Assistant Secretary	Date 1-6-16	Agency Secretary Matthew Rodriguez 	Date 1/6/16

Department of Finance Use Only

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

BCP Type: Policy Workload Budget per Government Code 13308.05

PPBA	Original Signed By: Ellen Moratti	Date submitted to the Legislature
------	--------------------------------------	-----------------------------------

Analysis of Problem

A. Budget Request Summary

The California Environmental Protection Agency (CalEPA) is requesting \$1.1 million in funding from multiple special funds, of which \$598,000 is for 4.0 permanent positions (4 PYs) and \$475,000 for maintenance costs annually to accommodate workload growth associated with increased demands for securing CalEPA's integrity, and privacy of confidential information. The classifications requested are: (1) Data Processing Manager III, (1) Data Processing Manager II, (1) Systems Software Specialist III (Technical), and (1) Systems Software Specialist II (Technical).

CalEPA and the boards, departments, and offices (BDO) need additional resources to assist with the increasing demand of two critical areas:

1. Information Security Program – implementation and enforcement of State/Federal laws, policies and mandates associated with securing information technology assets such as SAM Chapter 5300 and the U.S. EPA's Cross-Media Electronic Reporting Rule (CROMERR).
2. Cyber Security Management – implementation of technologies, processes, and practices designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access.

Over the last two years, these areas have proven vulnerable to breaches and intrusions. Details will be highlighted below, but without additional resources to support these two critical IT security areas systems that collect and provide information to the public, business partners, scientists, and environmentalists, as well as public officials will be continually compromised.

B. Background/History

BDO information systems contain personal and confidential information that if compromised, will result in a negative impact to CalEPA's ability to regulate entities and will diminish trust with the business community.

As the number of critical information technology assets for CalEPA and BDOs has increased over the years, CalEPA has not received an increase in the requisite information technology security support resources. The result is partial compliance of CalEPA systems with State and Federal information technology policies. In addition, security incidents have significantly risen in number and severity, which has impacted other information technology resources and projects.

CalEPA and BDO information technology systems are not fully compliant with the following SAM Chapter 5300 and CROMERR policy areas (this list does not cover all areas of non-compliance):

- Information security policies and procedures – SAM Chapter 5305.2 provides that each state entity establish appropriate administrative, operational and technical policies, standards, and procedures to maintain a standard of due care to prevent misuse.
- Risk and vulnerability assessments – SAM Chapter 5305.7 and 5330.1 provide that each state entity conduct risk and vulnerability assessments of its information systems.
- System Developer Security Testing – SAM Chapter 5315.4 provides that each state entity shall require system developers create and implement a security test and evaluation plan, as part of the system design and build.
- Vulnerability and Threat Management – SAM Chapters 5345 and 5355 provide that each state entity shall continuously identify and remediate vulnerabilities and detect malicious software before they can be exploited.
- Information Security Monitoring – SAM Chapter 5335.1 provides that each state entity is responsible for continuous monitoring of its network and other informational assets for signs of attack, anomalies, and suspicious or inappropriate activities.
- Information Security Incident Management – SAM Chapter 5340 provides that each state entity promptly investigate incidents to determine the cause, scope, and impact to prevent recurrence. CalEPA and BDOs have had a significant increase in the number of security incidents.

Analysis of Problem

- Information Asset Management – SAM Chapter 5305.5 prescribes that each state entity must establish and maintain an inventory which must include data classification of the information assets.
- U.S. EPA's Cross-Media Electronic Reporting Rule (CROMERR) policy – provides that entities that submit electronic information to U.S. EPA are compliant to ensure the enforceability of environmental programs and ensure the legal dependability of the electronic documents EPA systems receive. One system has received accreditation as being CROMERR compliant however no other CalEPA system has become compliant due to lack of resources. At least four other CalEPA systems need to be evaluated for CROMERR compliance.

Chapter 404, Statutes of 2010 (AB 2408) mandates each state agency appoint an information security officer to report to the state agency's chief information officer to ensure that the agency is complying with state policy. Several BDO information security officer appointments do not have industry standard accreditations in order to effectively implement and manage an information security program. The global leader in certifying and educating information security professionals is the International Information Systems Security Certification Consortium, Inc., (ISC)². (ISC)² strongly recommends (and most private organizations require) that Cyber Security staff become accredited as a Certified Information Systems Security Professional (CISSP). The CISSP certification is the ideal credential for those required to design, engineer, implement, and manage an organization's overall information security program.

CalEPA and BDOs have invested in shared technology and services. Shared technology includes networks, servers and security components. CalEPA does not have the required information security staffing to manage and oversee industry standard systems designed to protect and address the compliancy areas listed above. Some of these industry standard systems include:

- Next Generation Firewalls – In order to prevent or contain certain security incidents, staff must continuously oversee, audit, and confirm that firewall policies are being adhered to and the CalEPA shared infrastructure is continuously monitored.
- Advanced Persistent Threat (APT) Systems – CalEPA and BDOs have deployed APT technology in order to further protect CalEPA systems. Incident response plans and resources are needed to continuously monitor the APT system and remediate systems that are compromised.
- Web application Firewalls – CalEPA and BDOs have deployed web application firewall technology. This technology provides a significant increase in protection against common vulnerabilities and exposures to web application systems. The technology and associated SAM Chapter 5300 policy requires resources to implement website protection and continuously monitor and respond to alerts.
- Assessments – CalEPA and BDOs do not have adequate personnel to conduct the required assessments per SAM Chapter 5305.7 and 5330.1 to verify that system developers are complying with secure development principles.
- Data Classification – CalEPA and BDOs do not have the resources required to inventory existing systems for confidential and sensitive information. Data classification is important in order to provide an increase level of security and monitoring, to protect data from being stolen or compromised.

CalEPA and BDOs are unable to meet full compliance on the required security controls listed above, or manage the shared security technology investments that would play a vital role with respect to compliance and reducing security incidents. Security incidents have increased significantly across all of CalEPA at a time when the public and public officials are relying on CalEPA systems and data to make environmental policy, deal with quickly changing drought conditions, air quality legislation, and hazardous waste information. The justification section details the increase in security incidents and severity of the problem.

Analysis of Problem

C. State Level Considerations

CalEPA and BDOs provide confidential information to employees of other state departments such as the Board of Equalization (BOE), California Department of Public Health (CDPH), the Office of the Attorney General (OAG), local water and air districts, and Certified Unified Program Agencies (CUPAs). It is imperative that CalEPA establish policy and require external access to CalEPA systems be properly documented and assessed, so that industry standard secure connection methods are utilized and only the intended departments are the recipients of such confidential information.

The U.S. EPA established Cross-Media Electronic Reporting Rule (CROMERR) in order to improve the legal dependability of the electronic documents EPA systems receive. The California Secretary of State has introduced similar regulations (California Government Code section 16.5 and California Code of Regulations Title 2, Division 7, Chapter 10, Sections 22000-22006) to provide guidance towards identity proofing and creating a valid electronic (digital) signature. These regulations require that the digital signature is 1) unique to the person using it; 2) capable of verification; 3) under the sole control of the identity using it; and 4) linked to the data in such a manner that if the data is changed the digital signature is invalidated. Compliance is necessary for the legal dependability of the electronic documents EPA systems receive. CalEPA has several systems that exchange information with U.S. EPA.

D. Justification

AB 2408 explicitly prescribes each state agency appoint an information security officer to report to the state agency's chief information officer that the agency is complying with state policy.

Governor Brown's Executive Order B-34-15 requires all state departments and agencies comply with existing information security and privacy policies, and promote awareness of information security standards within their workforce.

CalEPA and its BDOs must bring systems into compliance and reduce the number of compromises from website breaches and associated downtime, potential lawsuits, and notification triggers (for compromised personally identifiable information). CalEPA must conduct new assessments on every website across CalEPA. CalEPA and its BDOs do not have the information security resources, training, and experience required for the oversight and guidance needed in performing security assessments. CalEPA and BDOs are mandated to certify compliance with SAM Chapter 5300 and, in the past, have been unable to meet 100% compliance.

CalEPA has been impacted by security breaches that have required BDOs notify individuals of potential compromise of personally identifiable information. Operations to websites have also been impacted and brought offline for remediation after being compromised. These breaches highlight the fact that once a system is compromised, the system must be removed from service and remediated before the system can be brought back online. The following recent examples related to security incidents and operational impacts were:

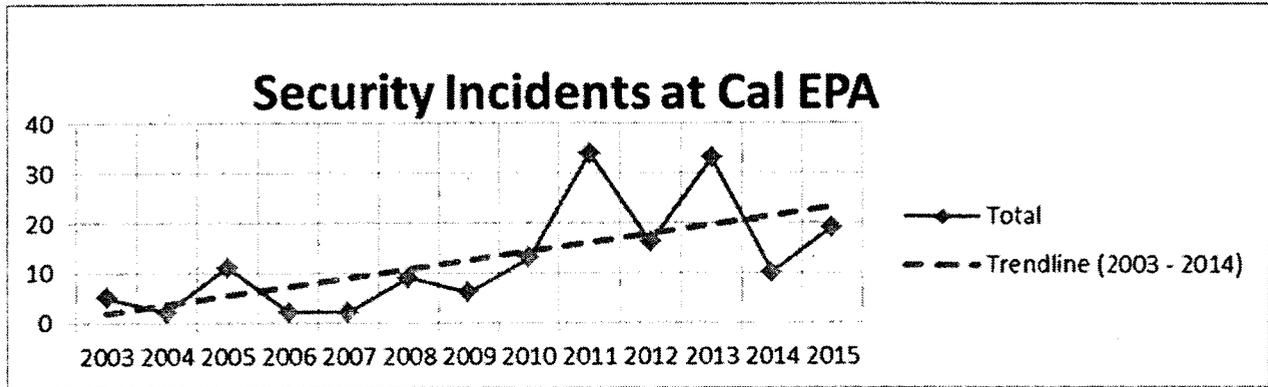
- Seven-week website outage – a press release was issued instructing the public to visit a specific website for information. Unfortunately, the website was taken offline immediately after the press release due to a compromise.
- Four-week outage on a training registration website – a training website was taken offline for 4 weeks due to compromise. BDO staff were redirected to handle training registrations manually.

Risk to CalEPA and BDOs may also extend to lawsuits if information that industry considers intellectual property, confidential business information, and trade secrets are compromised.

Security Incident response workloads have increased significantly across all of CalEPA (see figure 1). In June 2015, the FBI contacted the State Water Resources Control Board (Board) regarding six servers that may have been compromised by hackers from China. The Board and CalEPA staff had to stop their current assignments and provide the FBI with the requested server logs, server images, firewall logs, network, and other related information. CalEPA and the Board have been working diligently with the State Information Security Officer and other external security experts to conduct an internal investigation on this potential compromise. That investigation has revealed that a few of the

Analysis of Problem

systems in question by the FBI had known vulnerabilities that could have been leveraged to compromise the systems and gain access. However, our investigation results are inconclusive, because of the lack of logging information on the servers. Board staff decided to rebuild all of the systems, installing the latest patches and implementing new security measures to prevent any potential hacking from reoccurring. This incident generated additional workload to meet the FBI's requests detailed above and perform internal investigations. More work may be generated to provide additional server's logs, images and additional remediation activities.



Worldwide, the total cost of the average data breach increased 23% since 2013 with an average cost of \$3.79 million (according to Ponemon Institute's 2015 Cost of Data Breach Study, sponsored by IBM).

For CalEPA and BDOs to be effective in regulating industry, intellectual property and trade secrets are being taken with greater frequency. This requires an even greater emphasis on securing information to protect CalEPA and BDOs from a lawsuit due to either a single company or many companies losing control of confidential business information or trade secrets.

Currently CalEPA BDOs have an inconsistent standard for Information Security Officers, Information Security policies, risk assessments, application and system development, experience and priorities.

CalEPA has a shared infrastructure with over 100 websites, 500 servers, and 6000 workstations with no consistent standards for assessing and securing the systems. As CalEPA continues its regulatory roles, a variety of new and sensitive issues such as new Prop. 65 regulations, Water Board legislation, and environmental justice for Californians, raise the risk of attacks on systems and data integrity.

CalEPA systems have not been completely assessed to identify vulnerabilities. The few systems that have been assessed recently have highlighted critical vulnerabilities that required immediate remediation, as previously identified.

To reduce the previously outlined risks, CalEPA proposes to address the issue with resources for 2 major areas: Information Security Program Compliance (ISPC) and Cyber Security Management. The first major area, ISPC would focus on bringing the CalEPA systems into compliance with existing standards for Information Security and keeping systems in compliance. The second major area—Cyber Security Management—would manage information security practices to minimize information security risks going forward. The chart below identifies the resources needed to resolve the problems previously presented.

#	Tasks unaccomplished due to lack of resources	Resources needed
Information Security Program Compliance		
1	Information security policies and procedures – SAM Chapter 5305.2 compliance by implementing policy, oversight and assessments to validate compliance.	.25 PY
2	Risk and vulnerability assessments – SAM Chapter 5305.7	.25 PY

Analysis of Problem

	compliance	
3	System Developer Security Testing – SAM Chapter 5315.4 compliance	.25 PY
4	Vulnerability and Threat Management – SAM Chapter 5345 compliance	.25 PY
5	Information Security Monitoring – SAM Chapter 5335.1 compliance requires continuous monitoring and log analysis of information systems to identify baseline and abnormal conditions.	.25 PY
6	Information Security Incident Management – SAM Chapter 5340 compliance – Establishment of Incident Response and forensics teams to development intelligence when incidents happen to understand the root cause that allowed the infection and identify the appropriate preventative measures as corrective actions in order to reduce incidents.	.25 PY
7	Information Asset Management – SAM Chapter 5305.5 compliance	.25 PY
8	EPA's Cross-Media Electronic Reporting Rule (CROMERR) policy compliance	.5 PY
Cyber Security Management		
9	Firewall – resources to oversee, audit, and continuous monitoring.	.5 PY
10	Advanced Persistent Threat System –Implement and manage host based monitoring and protection for 6,000+ hosts.	.5 PY
11	Web application Firewall – Secure CalEPA and BDO public facing websites by implementing and managing a web application firewall and continuously monitoring.	.25 PY
12	Assessments – resources to conduct assessments and ensure that system developers are developing with secure application development principles.	.25 PY
13	Data Classification – resources to assess data classification systems and procure a system that automates the classification of data in structured (database) and unstructured (file) systems to identify systems containing confidential information, trade secrets and intellectual property.	.25 PY
	Total	4 PY

Each of these tasks is required by the State Administrative Manual Chapter 5300. These resources would improve protection for the CalEPA information systems by bringing CalEPA systems into compliance with current information security standards. This, combined with additional security management practices is the best way to reduce information security risks at the CalEPA efficiently.

E. Outcomes and Accountability

CalEPA is seeking positions with the classifications necessary to attract experienced and certified information security professionals that can assume ISO roles for BDOs when needed and provide the high level authority and expertise for the shared services infrastructure and BDO policies, auditing, forensics, assessments, risk management, and secure application development guidance and oversight. Accountability will be provided by identifying clear deliverables addressing each of the challenges described in the background/history section.

Analysis of Problem

In an effort to address the ever-changing demands of securing CalEPA's confidential, sensitive, and personal information, CalEPA and BDOs have established measurable outcomes for each of the efforts listed in the justification. Reports on all metrics below will be provided to the BDO CIOs and Agency Information Officer (AIO).

Projected Outcomes

Workload Measure	CY	BY	BY+1	BY+2	BY+3	BY+4
	0	Validate 1 st BDO	Validate 2 nd and 3 rd BDO	Validate 4 th and 5 th BDO	Validate all CalEPA and BDOs	Continuous validation and auditing
Risk and Vulnerability Assessments	0	Establish policy on risk and vulnerability assessments	Validate compliance with policy			
System Developer Security Testing Compliance	0	Provide Guidance and training to perform assessments	Validate development teams conducting assessments	Continuous audit and validation	Continuous audit and validation	Continuous audit and validation
Vulnerability and Threat Management Compliance	0	APT system rollout to 6000 hosts	APT system rollout to 6000 hosts	APT system rollout to 6000 hosts	APT system rollout to 6000 hosts	APT system rollout to 6000 hosts
Information Security Monitoring	0	Implement information security monitoring policy, process and procedures	Ensure the resource in place is following monitoring process and procedures	Ensure the resource in place is following monitoring process and procedures	Ensure the resource in place is following monitoring process and procedures	Ensure the resource in place is following monitoring process and procedures
Information Security Incident Management	0	Establish Incident response process and procedures	Establish incident response and forensics teams	Validate incident response process compliance	Validate incident response process compliance	Validate incident response process compliance
Information Asset Management	0	Establish policy for data classification	Validate compliance with policy			
CROMERR Compliance	0	Identify systems needing CROMERR compliance	Identify Project plans to bring systems into compliance	Execute project plans	Execute project plans	Execute project plans
Next Generation Firewall	0	Continuous firewall monitoring	Continuous firewall monitoring	Continuous firewall monitoring	Continuous firewall monitoring	Continuous firewall monitoring
Advanced Persistent Threat system	0	Implement for all CalEPA	All (6,000+) hosts protected			
Web Application Firewall	0	Implement protection	All (50+) websites	All (50+) websites	All (50+) websites	All (50+) websites

Analysis of Problem

		for 50+ websites				
Risk and Vulnerability Assessments	0	Conduct assessments of first 50 systems	Conduct assessments of systems 51 - 100	Rolling and continuous assessment schedule	Rolling and continuous assessment schedule	Rolling and continuous assessment schedule
Data Classification	0	Evaluate tools to automate data classification	Implement data classification system	Validate all systems have continuous data classification	Validate all systems have continuous data classification	Validate all systems have continuous data classification

F. Analysis of All Feasible Alternatives

Alternative #1 – Approve funding of \$598,000 for 4 permanent positions (4 PY's), and \$475,000 for ongoing maintenance of the information security solutions

This alternative allows CalEPA to meet its measurable goals and objectives, and increased workload demands by shifting from reacting to security incidents to proactively managing risks. This alternative provides resources to bring CalEPA into compliance and implement required IT security policy and IT controls, as well as mitigate security risks. Risk mitigation limits breaches in which confidential, sensitive, and personal or trade secret information is exposed and/or misused. This alternative could result in significant savings/avoided costs by reducing IT security risks and potential related litigation.

Alternative #2 – Approve funding of \$2,075,000 per year for consulting services, and \$475,000 for ongoing maintenance of the information security solutions.

This alternative provides resources to CalEPA to enter into a contractual agreement with an independent consulting company to implement required security policies and controls, and mitigate the security risks without adding new positions, but at a much higher cost. This alternative also introduces a higher degree of risk associated with providing contract personnel with access to CalEPA's environment which contains CBI, IP, and regulated entity trade secrets. The cost for this alternative would equal or exceed \$2,075,000 to fully meet CalEPA's needs.

Alternative #3 – Status Quo

This alternative would continue high risk for CalEPA information and information assets and risk an ever increasing impact of security breaches to hosts, websites, and confidential information. As the information security incidents have increased over the years, resources have had to focus on incident response, taking those resources away from planning, projects, and supporting CalEPA programs.

G. Implementation Plan

Major Milestones for implementing the proposed solution include:

Task Name	Duration	Start	Finish
Funding (Budget Enactment, Funding)	2 months	7/1/2016	8/30/2016
Hiring of Primary Information Security Officer to fully implement information security program – Duties: Implementing overarching policy for all of CalEPA, ensuring compliance with oversight and verifying by performing risk and compliance assessments.	2 months	9/1/2016	10/30/2016
Hiring of Secondary Information Security Officer. The Primary and Secondary Information Security Officers	2 months	11/1/2016	12/30/2016

Analysis of Problem

will fulfill all compliance duties as listed in the "Projected Outcomes" chart in section E.			
Hiring of Primary and Secondary Cyber Security Specialists to fulfill all Cyber Security Management Responsibilities in the "Projected Outcomes" chart in section E. Agency Information Security Office hires resources to achieve the goals and outcomes in section E.	2 months	1/1/2017	2/28/2017
The Information Security Office will provide the following: A) Continuous Compliance monitoring, oversight, policy, guidance, and risk assessments B) Cyber Security Management to ensure the technical controls are in-place for all CalEPA and BDO systems to prevent compromise of confidential data or systems.	Continuous	3/1/2017	n/a

H. Supplemental information

This proposal also requests the following maintenance costs per year:

#	Item	Cost
1	Website Protection maintenance costs	\$50,000
2	Host based protection maintenance costs	\$50,000
3	Risk Assessments from contracted resource	\$250,000
4	Firewall maintenance costs	\$70,000
5	Information Security and Awareness Training	\$20,000
6	Onsite class for secure application development principles	\$35,000
	Total	\$475,000

I. Recommendation

Alternative #1 is the recommended solution. This alternative will allow CalEPA to comply with IT security related laws, regulations, and policies. Furthermore, CalEPA will reduce the risks from potential lawsuits, vulnerable websites, and future data breaches while providing the training and guidance needed to all CalEPA BDOs for the handling of confidential and sensitive information such as trade secrets, intellectual property, and confidential business information. Vulnerabilities will be remediated thereby allowing information technology professionals to shift from incident response to completing projects and providing accurate information to the public and public officials.

BCP Fiscal Detail Sheet

BCP Title: Cyber Security Workload Growth

DP Name: 0555-101-BCP-DP-2016-GB

Budget Request Summary

	FY16					
	CY	BY	BY+1	BY+2	BY+3	BY+4
Positions - Permanent	0.0	4.0	4.0	4.0	4.0	4.0
Total Positions	0.0	4.0	4.0	4.0	4.0	4.0
Salaries and Wages						
Earnings - Permanent	0	343	343	343	343	343
Total Salaries and Wages	\$0	\$343	\$343	\$343	\$343	\$343
Total Staff Benefits	0	159	159	159	159	159
Total Personal Services	\$0	\$502	\$502	\$502	\$502	\$502
Operating Expenses and Equipment						
5301 - General Expense	0	8	8	8	8	8
5302 - Printing	0	4	4	4	4	4
5304 - Communications	0	8	8	8	8	8
5320 - Travel: In-State	0	16	16	16	16	16
5322 - Training	0	4	4	4	4	4
5324 - Facilities Operation	0	40	40	40	40	40
5340 - Consulting and Professional Services -	0	475	475	475	475	475
5346 - Information Technology	0	16	12	12	12	12
Total Operating Expenses and Equipment	\$0	\$571	\$567	\$567	\$567	\$567
Total Budget Request	\$0	\$1,073	\$1,069	\$1,069	\$1,069	\$1,069

Fund Summary

Fund Source - State Operations						
0028 - Unified Program Account	0	216	215	215	215	215
0106 - Department of Pesticide Regulation Fund	0	76	76	76	76	76
0115 - Air Pollution Control Fund	0	259	258	258	258	258
0387 - Integrated Waste Management Account,	0	138	138	138	138	138
0439 - Underground Storage Tank Cleanup Fund	0	384	382	382	382	382
Total State Operations Expenditures	\$0	\$1,073	\$1,069	\$1,069	\$1,069	\$1,069
Total All Funds	\$0	\$1,073	\$1,069	\$1,069	\$1,069	\$1,069

Program Summary

Program Funding						
0340 - Support	0	1,073	1,069	1,069	1,069	1,069
Total All Programs	\$0	\$1,073	\$1,069	\$1,069	\$1,069	\$1,069

