

STATE OF CALIFORNIA
Budget Change Proposal- Cover Sheet
 DF-46 (REV 03/13)

Fiscal Year 2014/15	BCP No. 5	Org. Code 7730	Department Franchise Tax Board	Priority No. 5
------------------------	--------------	-------------------	-----------------------------------	-------------------

Program Tax Programs	Element N/A	Component N/A
-------------------------	----------------	------------------

Proposal Title
Data Security

Proposal Summary

The Franchise Tax Board (FTB) is requesting \$2.6 million and 7 positions in 2014/15 to accommodate workload growth and the implementation of new tools associated with increased demands for securing FTB's critical assets and ensuring confidentiality and privacy of taxpayer information.

- FTB is requesting seven positions and \$800,000 in 2014/15 to meet increased workload demands for securing FTB's critical assets and ensuring confidentiality and privacy of taxpayer information.
- FTB is also requesting one-time funding of \$1.8 million in 2014/15 and ongoing funding of \$546,000 and two positions in 2015/16 to procure and install a Data Security Monitoring and Auditing system that will provide a comprehensive data audit and protection suite for preventing data theft, strengthening data privacy, and managing user access rights. This latter component of the request is supported by a Feasibility Study Report (FTB FSR 13-02) as approved by the Government Operations Agency on July 12, 2013, and pending approval by the Department of Technology.

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 No	Code Section(s) to be Added/Amended/Repealed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	Date
---	----------------	------

For IT requests, specify the date a Special Project Report (SPR) or Feasibility Study Report (FSR) was approved by the California Technology Agency, or previously by the Department of Finance.

FSR SPR Project No. FTB FSR 13-02 Date: Pending Approval

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
Department Director	Date	Department Director	Date

Pending Board Approval

Department of Finance Use Only

Additional Review: Capital Outlay ITCU FSCU OSAE CALSTARS Technology Agency

BCP Type: Policy Workload Budget per Government Code 13308.05

PPBA Date submitted to the Legislature

Fiscal Summary
(Dollars in thousands)

BCP No 5	DATE August 14, 2013	Proposal Title: Data Security	PROGRAM Tax Programs
-----------------	--------------------------------	---	--------------------------------

	Positions			FY 2013/14	FY 2014/15	FY 2015/16
	CY	BY	BY + 1	CY	BY	BY + 1
Total Salaries & Wages /1	.0	7.0	9.0	\$ 0	\$ 479,000	\$ 633,000
Total Staff Benefits /2				\$ 0	\$ 214,000	\$ 280,000
Total Personal Services				\$ 0	\$ 693,000	\$ 913,000

Operating Expenses and Equipment

General Expense /3	\$ 0	\$ 14,000	\$ 10,000
Printing	0	0	0
Communications /4	0	5,000	6,000
Postage	0	0	0
Travel-In-State	0	0	0
Travel Out-of-State	0	0	0
Training /5	0	20,000	0
Facilities Operations /6	0	20,000	0
Utilities	0	0	0
Cons & Prof Svs - Interdept'l	0	0	0
Cons & Prof Svs - External /7	0	37,000	0
Data Center Services	0	0	0
Information Technology /8	0	1,761,000	332,000
Equipment	0	0	0
Other/Special Items of Expense	0	0	0
Total Operating Expense & Equipment	\$ 0	\$ 1,857,000	\$ 348,000

TOTAL STATE OPERATIONS EXPENDITURES

\$ 0 \$ 2,550,000 \$ 1,261,000

Fund Source

	<u>Item No.</u>					
	Org	- Ref	- Fund			
General Fund	7730	001	0001	\$	0	\$ 2,550,000 \$ 1,261,000
					0	0 0
					0	0 0
					0	0 0
					0	0 0
					0	0 0
					0	0 0
					0	0 0
Totals				\$	0	\$ 2,550,000 \$ 1,261,000

Total Local Assistance Expenditures

\$(0) \$(0) \$(0)

Fund Source

	<u>Item No.</u>					
	Org	- Ref	- Fund			
	7730	001	0001	\$	0	\$ 0 \$ 0
					0	0 0
					0	0 0
					0	0 0
					0	0 0
					0	0 0
Totals				\$	0	\$ 0 \$ 0

Grand Total, State Operations and Local Assistance

\$ 0 \$ 2,550,000 \$ 1,261,000

- /1 Itemized positions by classification on the Personal Services Detail worksheet.
- /2 Benefit detail on the Personal Services Detail worksheet.
- /3 General Expense @ \$910 per position. Plus minor equipment @ \$1184 per new position.
- /4 Communication costs @ \$644 per position.
- /5 One-time system training \$20,000
- /6 Facilities Costs: build new stations in security suite
- /7 One Time solution provider Data Security system contract services \$37,000
- /8 One-Time Costs of Data Security system @ \$1,742,000 with on going maintenance of \$318,000, Hardware and Software for new positions

PERSONAL SERVICES DETAIL
(Whole Dollars)

BCP No 5	DATE August 14, 2013	Proposal Title: Data Security	PROGRAM Tax Programs
-----------------	--------------------------------	---	--------------------------------

Positions		Positions			Salary Range	CY	Dollars	
		CY 2013/14	BY 2014/15	BY + 1 2015/16			BY	BY + 1
Administrative Services Division								
Staff Serv Analyst Gen - Rg B	PERM	0.0	1.0	1.0	\$ 3,050 \$ 3,819	\$ 0	\$ 41,000	\$ 41,000
Sys Software Spec II Tech	PERM	0.0	4.0	5.0	\$ 5,561 \$ 7,310	\$ 0	\$ 309,000	\$ 386,000
Staff Info Sys Analyst Spec	PERM	0.0	1.0	1.0	\$ 5,065 \$ 6,660	\$ 0	\$ 70,000	\$ 70,000
Assoc Gvmtl Prog Analyst	PERM	0.0	1.0	1.0	\$ 4,400 \$ 5,508	\$ 0	\$ 59,000	\$ 59,000
Total Administrative Services Division		.0	7.0	8.0		\$ 0	\$ 479,000	\$ 556,000
Adjust for Part Year Positions		.0	.0	.0				
Net Positions		.0	7.0	8.0				
Technology Services Division								
Sys Software Spec II Tech	PERM	0.0	0.0	1.0	\$ 5,561 \$ 7,310	\$ 0	\$ 0	\$ 77,000
Total Technology Services Division		.0	.0	1.0		\$ 0	\$ 0	\$ 77,000
Adjust for Part Year Positions		.0	.0	.0				
Net Positions		.0	.0	1.0				
Total Salaries and Wages								
	Positions	.0	7.0	9.0		\$ 0	\$ 479,000	\$ 633,000
	Part Yr Adj	.0	.0	.0				
	Net Positions	.0	7.0	9.0				

Staff Benefits Detail

	2013/14	2014/15	2015/16
OASDI /9	\$ 0	\$ 30,000	\$ 40,000
Health/Dental/Vision Insurance /10	0	76,000	98,000
Retirement - Miscellaneous /11	0	98,000	130,000
Worker's Compensation /12	0	3,000	3,000
Industrial Disability Leave/13	0	0	0
Non Industrial Disability Leave /14	0	0	0
Unemployment Insurance /15	0	0	0
Medicare /16	0	7,000	9,000
Total Staff Benefits	\$ 0	\$ 214,000	\$ 280,000

9/ For permanent and overtime, 6.2% of salary.

10/ Health - For Permanent \$10,150 per position; Dental - For permanent \$587 per position;

Vision - for permanent \$106 per position.

11/ For permanent, 20.503% of salary.

12/ 0.55% of salary for permanent.

13/ 0.03% of salary for permanent.

14/ 0.06% of salary for permanent.

15/ 8.8% of salary for temporary help.

16/ 1.45% of salary for permanent.

**FISCAL YEAR 2014/15
 SUPPLEMENTAL INFORMATION
 (\$ in Thousands)**

Identify all proposed items which fit into the categories listed below.

	<u>Current Year</u>	<u>Budget Year</u>	<u>Budget Year + One</u>
<u>Proposed Equipment</u>			
	\$ 0	\$ 0	\$ 0
Total	<u>\$ 0</u>	<u>\$ 0</u>	<u>\$ 0</u>
<u>Proposed Contracts</u>			
Solution Provider For Data Security System	\$ 0	\$ 37	\$ 0
Total	<u>\$ 0</u>	<u>\$ 37</u>	<u>\$ 0</u>
<u>One-Time Costs</u>			
General Expense - Minor Equipment (chair, calculator, telephone, data connection)	\$ 0	\$ 4	\$ 2
Training	0	20	0
Information Technology		1,429	6
Total	<u>\$ 0</u>	<u>\$ 1,453</u>	<u>\$ 8</u>
<u>Future Savings</u>			
	\$ 0	\$ 0	\$ 0
Total	<u>\$ 0</u>	<u>\$ 0</u>	<u>\$ 0</u>
<u>Full-Year Cost Adjustments</u>			
	\$ 0	\$ 0	\$ 0
Total	<u>\$ 0</u>	<u>\$ 0</u>	<u>\$ 0</u>
<u>Facilities/Capital Costs</u> - indicate one-time or ongoing			
One-time facility cost to build new stations in security suite	\$ 0	\$ 20	\$ 0
Total	<u>\$ 0</u>	<u>\$ 20</u>	<u>\$ 0</u>

Analysis of Problem

A. Proposal Summary

The Franchise Tax Board (FTB) is requesting \$2.6 million and 7 positions in 2014/15 to accommodate workload growth and the implementation of new tools associated with increased demands for securing FTB's critical assets and ensuring confidentiality and privacy of taxpayer information.

- FTB is requesting seven positions and \$800,000 in 2014/15 to meet increased workload demands for securing FTB's critical assets and ensuring confidentiality and privacy of taxpayer information.
- FTB is also requesting one-time funding of \$1.8 million in 2014/15 and ongoing funding of \$546,000 and two positions in 2015/16 to procure and install a Data Security Monitoring and Auditing system that will provide a comprehensive data audit and protection suite for preventing data theft, strengthening data privacy, and managing user access rights. This latter component of the request is supported by a Feasibility Study Report (FTB FSR 13-02) as approved by the Government Operations Agency on July 12, 2013, and pending approval by the Department of Technology.

B. Background/History

FTB employs a 'Defense-in-Depth' strategy to protect the confidential information entrusted to us by our customers. Defense-in-Depth is a widely accepted security strategy where multiple layers are in place throughout an information technology system to protect it from accidental or intentional unauthorized access, modification, destruction and misuse. FTB has in place multiple layers of protection mechanisms, oversight, procedures and policies for the purpose of ensuring the confidentiality, integrity and availability of FTB's IT systems and assets. The sole purpose is to prevent security breaches, fraud, and detect and respond to an attack, thereby reducing and mitigating the consequences associated with a breach of confidential information.

FTB's Chief Security Officer is responsible for the oversight and management of all aspects of information security. This program is managed by Information Security and Oversight Section. The objective of the information Security program is to:

- Protect FTB's information and information processing assets which also includes prevention and detection of fraud, inappropriate use/access and physical damage or losses.
- Manage vulnerabilities within the information processing infrastructure.
- Manage threats and incidents impacting FTB's information resources.
- Assure through oversight, policy, standards and procedures the appropriate use of FTB information resources.

The Chief Security Officer is also responsible for the physical security of our worksites. This program, managed by the Worksite Security Section, is responsible for the physical security of FTB employees, assets and data (including vendors and visitors). This program objective is to:

- Ensure the protection of employees, assets and data through oversight and enforcement.
- Prevent unauthorized building accesses through oversight, administration and maintenance of the physical access (badging system) and alarm monitoring system for the campus and all FTB offices throughout the nation.
- React quickly to threats, physical attacks and/or vandalism through oversight, administration and maintenance of advanced security technology, including closed circuit television camera systems (CCTV), access control and alarm monitoring systems and oversight of a large security officer force.
- React quickly to incidents that impact FTB's physical security for assets and employees.
- Ensure the necessary resources are available to protect FTB physical assets and employees through active oversight, management and administration of the Security Guard contract.
- Ensure appropriate and up to date policies, procedures and practices are in place to protect FTB's employees, assets and data.
- Conduct and oversee appropriate and timely enforcement activities.

Analysis of Problem

FTB's limited capability to monitor, log, alert, and audit data access events and transactions as well as a shortage of security staff has put the department at risk of non compliance with state and federal requirements and mandates. A security breach of confidential taxpayer information or loss of Internal Revenue Service (IRS) data would negatively impact FTB's mission and the state's ability to collect revenue.

Resource History (Dollars in thousands)

Program Budget	2008-09	2009-10	2010-11	2011-12	2012-13
Authorized Expenditures	3,568	3,239	3,856	4,005	4,396
Actual Expenditures	2,990	3,212	3,677	3,971	4,081
Authorized Positions	35	34	37	38	38
Filled Positions	30	33.8	34.1	35.9	38
Vacancies	5	.2	2.9	2.1	0

C. State and Federal Considerations

FTB provides access to information to employees of other state departments such as the Board of Equalization (BOE), Employment Development Department (EDD), and the Department of Child Support Services (DCSS). Interagency Agreements and FTB policy requires FTB to log and audit external accesses to FTB systems. In addition to the confidential information FTB obtains directly from taxpayers in the course of administering the California Revenue and Taxation code, FTB's databases also store confidential and sensitive data it receives through a number of Interagency Agreements and Memorandums of Understanding (MOU) with other state agencies.

FTB also receives confidential taxpayer information from the IRS. The data that IRS provides is critical to the success of FTB's ability to meet its obligation of collecting the right amount of tax and closing the tax gap. As part of the agreement, IRS requires that FTB complies with the IRS Publication 1075, "*Tax Information Security Guidelines for Federal, State, and Local Agencies and Entities*." The IRS requires that agencies conduct security assessments of information systems to determine if security controls are implemented correctly, including auditing users to ensure that only those who have a "need to know" access federal data. Failure to adequately protect this data could result in the refusal of the IRS to provide the data, which would have a substantial negative impact on State revenue.

This proposal supports FTB's mission to responsibly manage the resources allocated to us. This proposal also supports FTB's Strategic Plan foundational principle to protect taxpayer information and privacy. Providing FTB with the resources for managing this workload is representative of the commitment that the state of California places on protecting taxpayer information and privacy.

D. Justification

Security Workload Growth

FTB is requesting seven positions and \$800,000 in 2014/15 to meet increased demands for securing FTB's critical infrastructure and assets. These resources are critical for maintaining public trust and encouraging self compliance with tax laws by ensuring the confidentiality, integrity, and availability of FTB's information technology systems and the information they contain.

Cyber security threats continue to grow and mutate as societal changes and information technology trends shift and expand. FTB must continue to prepare for and defend against these constantly evolving threats. Additionally, the increase in dependence on cloud computing solutions, mobile computing devices in the workplace, and the growing volumes of data we maintain that could be used for profit by would be thieves, inside and outside the organization, requires constant oversight and monitoring.

Analysis of Problem

FTB's critical infrastructure and assets include but are not limited to (numbers are approximate) 7,000 desktop and notebook computers, 200 mobile devices, 1,500 servers and appliances, one large mainframe computer, 2,500 software applications, and 3,200 databases containing 381,000 tables and 216 billion data records. Information Security staff must oversee, monitor, certify, audit and otherwise secure the changes to these and changes resulting from other emerging IT services and assets. In 2012/13, FTB's systems and applications supported the collection of approximately \$75 billion in revenue.

Information Security Oversight Specialist (one position)

The FTB must comply with many federal and state requirements regarding information security in order to protect the information assets entrusted to it. Information Security Oversight Specialists are the department's information security subject matter experts, providing support and oversight to departmental projects, task forces, and initiatives. Staff consults with departmental program areas and project teams to ensure compliance with Information Security Policies and industry best practices for system and network design issues. This position is critical in order to provide security oversight to ensure the protection of FTB's information systems. These systems contain vast amounts of confidential and sensitive data that if compromised, will negatively impact the collection of tax revenue. The shortage of staff has resulted in the inability to meet the demands for project oversight and risk mitigation. For example, the Senior Information Security Specialist averages 40 conflicting meetings per month where Information Security Oversight Specialist presence is mandatory to ensure the necessary security requirements and compliance are in place. Not being present, causes delays in security requirement implementation and causes project delays and unnecessary risk to FTB systems and data. It also puts the department at risk of not being in compliance with state and federal requirements and mandates.

Intrusion Detection Response Specialist (one position)

The Intrusion Detection Response Team is responsible for monitoring specific computers and networks to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). Additionally, they provide high-level expertise in the discipline of computer and network security, vulnerability assessment, intrusion detection, virus detection, and hacking methodologies. They research current security threats, zero day attacks, and industry trends as they relate to the improvement of FTB's intrusion detection security technology. This position will communicate with network and system administrators to resolve alerts generated by the Intrusion Detection Response System (IDRS). With the substantial upgrades currently occurring to our technology applications, it is estimated that 40 new Host Intrusion Detection Sensors (HIDS) will be required. Currently, we have 67 HIDS installed in our production environment; therefore we estimate the resulting 100 or more HIDS will increase security events by 40 percent. This position will be required to monitor and analyze alerts of the additional agents and perform maintenance of all of these sensors. It is critical that FTB have the resources necessary to monitor for potential intrusions. If FTB does not have the resources to fully evaluate all of the alerts this puts FTB systems at risk of a security breach. The evolution of hybrid attacks utilizing multiple pathways to breach security infrastructure has highlighted the need for organizations to defend themselves against a constantly shifting threat. If even a single attack is successful, FTB could suffer significant loss of revenue if production lines were to go dark and tax processing came to a halt. Methods of attack have become increasingly more sophisticated; a more proactive approach is required to defend against new and evolving threats.

Information Security Compliance Specialist (one position)

This position will review and certify new FTB applications to ensure that they are in technical compliance with FTB security policies. This position will perform detailed technical analysis of vulnerabilities identified and provide detailed reports to the application developer(s). Not identifying these vulnerabilities could put FTB critical assets at risk. The shortage of staff has resulted in the inability to perform a detailed review of all of the applications being implemented to ensure that they are in compliance with FTB security policies. Currently, we can only identify the most critical functions of the application to perform a security review. This type of methodology is not recommended due to the criticality of the data and increased exposure to attacks of critical FTB assets.

Penetration Testing Specialist (one position)

Penetration Testing Specialists are responsible for conducting formal tests on web-based applications, networks, and other types of computer systems on a regular basis to ensure the security of the application. Currently for the EDR project, this function is performed by the Service Provider (SP) and this workload will need to be redirected to FTB as the SP transitions the work. If the position is not granted, FTB will not be

Analysis of Problem

able to perform penetration testing on all existing FTB web based applications – particularly the external taxpayer folder implemented as part of the EDR project. Since these are public facing applications, detailed application penetration testing must be routinely performed on a continual basis.

Internal Investigations Team (two positions)

The number of complex information security investigative audits has increased significantly over the last few years to a point where it has become increasingly difficult for staff to find time to conduct the core routine audit workload. The increase in the number of complex investigative audits has resulted in longer timeframes for case resolution with each case requiring immediate and active involvement from Security staff, putting other workloads on hold. This is not necessarily because investigative audits are more important but rather because attention to the investigation is driven by urgency, risk, complex coordination with internal and external entities and other circumstances beyond our control. Other workloads are mandated by information security requirements and are also equally important to protecting FTB's critical information assets. These two positions allow us to manage a broad spectrum of workloads.

FTB also has seen a dramatic increase in harassment claims (FTB's Zero Tolerance Policy – threats, intimidation, etc) that require a thorough investigation to determine the appropriate outcome. This workload has increased significantly and has grown more complex. From 2008 to 2010, the number of harassment investigations averaged 20 per year. In 2011, the number of harassment claims filed jumped to 50, in 2012, the number of claims rose to 60 and in 2013; we are on track for approximately the same proportional increase of additional cases. These workloads are mandatory in nature and must be addressed regardless of available resources. Therefore as these workload numbers and complexities increases, it decreases FTB's ability to appropriately address critical on-going workloads that ensure that critical data entrusted to FTB is protected.

In addition to the above mentioned workload growth, effective July 1, 2013, FTB adopted a centralized approach for our internal investigation processes that maximized our resources and subject matter experts. Prior to July 1, 2013, an Information Security Auditor would gather the facts and provide a timeline and supporting information of an internal investigative audit to the responsible FTB supervisors and managers who would subsequently interview the employee(s) about their alleged misconduct if deemed necessary. There were many issues and problems with this approach. FTB Executives approved the change to shift the entire responsibility for internal investigations to the Information Security Audit and Internal Investigations Unit (new name) to mitigate risks to the state and FTB, and to continue ensuring due process was allowed to the employee being investigated for an alleged misconduct. The result is a more efficient, consistent and legal internal investigations process because information security audit staff are trained in investigative and interrogations techniques, are subject matter experts in FTB policy, laws and regulations related to information security and work routinely with FTB legal and human resources subject matter experts and law enforcement entities. FTB supervisors and managers still have a key role in the process as subject matter experts on their specific business processes and employees.

The Internal Investigator will be responsible for conducting administrative investigations of possible inappropriate, illegal, and/or fraudulent activities by internal staff, vendors or business partners. The Internal Investigation Intake Specialist will provide support to the Internal Investigators and will be responsible for intake case management including preliminary analysis and case responsibility, responding to customer inquiries for potential administrative cases, and assisting in obtaining facts and evidence to support the case for the Internal Investigator.

If these positions are not granted, it will decrease FTB's ability to timely address internal threats to FTB information assets, timely report information disclosures to taxpayers, prevent multiple unauthorized accesses, and continued misconduct. Because the information security audit program is a deterrent to inappropriate activity, FTB could also see an increase in misconduct and fraudulent activities, loss of state revenue and potentially the termination of our data sharing agreement with the IRS and other business partners.

Worksite Security Section (one position)

Worksite Security Section is responsible for oversight, administration and maintenance of FTB's badging system and closed circuit television camera systems (CCTV). These systems collect and store massive amounts of data. Currently, the badging system and CCTV data are only reviewed to support ongoing investigations where an incident or issue has been reported. However, while performing reviews for specific incidents staff has identified other anomalies. Recently selected portions of the data have been

Analysis of Problem

reviewed on a routine basis, which has uncovered access issues and employee misconduct that would have gone unnoticed and unreported.

This position will perform routine audits of the CCTV and badging systems. Having a dedicated resource to review and audit this data will significantly increase FTB's ability to stay in a proactive mode and to acknowledge and respond appropriately to issues of misconduct or that represent a threat to the department. This position will also provide support to the Internal Investigations Team to assist with the reduction of backlogs as well as help reduce the overall time for completing investigations. This will help by keeping small issues from growing into larger or more complex issues when they are left unresolved for longer periods of time. If this position is not granted, it will decrease FTB's ability to timely monitor for policy violations and criminal activities (theft, vandalism, etc). This type of activity has the potential for loss of revenue to the state.

Data Security Tool

This proposal includes one-time funding of \$1.8 million in 2014/15 and ongoing funding of \$540,000 and two positions in 2015/16 to procure and install a Data Security Monitoring and Auditing system that will provide a comprehensive data audit and protection suite for preventing data theft, strengthening data privacy, and managing user access rights. This component of the request is supported by a Feasibility Study Report (FTB FSR 13-02) as approved by the Government Operations Agency on July 12, 2013, and pending approval by the Department of Technology.

The 2011 IRS safeguard review directs FTB to pro-actively monitor real-time user activities on our databases and file servers. FTB currently does not have the capability to monitor, log, alert, and audit data access transactions and determine who accessed which record/file and what action they took on the record/file in real-time on an enterprise level and heavily rely on a manual process. However, current resource limitations and limitation of tools has jeopardized FTB from applying the desired level of scrutiny to system accesses to mitigate risks associated with unauthorized accesses to our critical data. Enhancing this capability is of vital importance since database and file servers are the largest target of unauthorized access, with the highest yield of records (database and file servers account for the majority of records lost from all categories per Verizon's "2011 Data Breach Investigations Report"). In addition, the capability to monitor real-time user activities is required in order to be in compliance with IRS safeguard audit requirements. FTB currently has no proactive real-time data monitoring and reporting and no consistent verifiable audit trail for data access in compliance with state and federal statutes and regulations.

Because FTB lacks a robust automated system to monitor real-time activity, a manual, labor-intensive process is often required to analyze massive amounts of logs to ensure any reported incident is resolved in a timely manner. With this process, if a data breach incident occurs, FTB might not have sufficient information to detect or conduct a complete and accurate forensic analysis in a timely manner. The manual process does not provide proactive, real-time data monitoring and reporting, and can only be conducted after an incident has occurred. The manual process does not provide consistent verifiable audit trails in compliance with federal statutes and regulations, and does not offer an enterprise tool to provide data baseline standards and enforcement.

Without remediation of the current situation, FTB runs the risk of a data breach that could expose confidential records and could be costly for the state to rectify. According to a study from Ponemon Institute, the average cost of a data breach incident was \$5.5 million in 2011 (the average data breach cost per record is \$194). A data breach at the University of South Carolina in January 2011 exposed 31,000 records on the Internet and will cost the university more than \$6 million.

A data breach at the South Carolina Department of Revenue discovered in October 2012 included approximately 3.8 million Social Security numbers, 387,000 credit and debit card numbers and 657,000 business tax filings. According to a January 6, 2013 article posted on TheState.com, the price tag for the breach is \$20 million and climbing.

To reduce the risk of a data breach and be in compliance with departmental policy, as well as federal statutes and regulations, FTB must implement tighter risk control measures over its information systems, including a verifiable audit trail. With a data security solution tool in place, FTB mitigates the risk of these potential costly threats to the confidential data we are entrusted with.

Analysis of Problem

E. Outcomes and Accountability

In an effort to address the ever-changing demands of securing FTB's confidential, sensitive, and personal information, FTB Executive Management has established the Information Security Audit and Compliance Monitoring Units under the direction of FTB's Chief Security Officer (CSO). The CSO reports directly to the Executive Officer on all matters related to the department's compliance with policies and procedures regarding the security of critical assets. The implementation and on-going progress of the initiatives addressed in the BCP will be monitored by the CSO who will provide regular reports to Executive Management regarding the challenges and successes of securing one of FTB's most critical assets—confidential, sensitive, and personal information.

Projected Outcomes (Technology Services Division)

(In Hours)

Workload Measure	2012-13	2013-14	2014-15	2015-16
Upgrading database management systems (DBMS) software, applying database management systems software fixpak and ongoing maintenance of the software including various system requirements in order for the software to operate.	14,496	14,024	14,024	14,731
Installing and configuring a database management system, and troubleshooting issues and ongoing maintenance of the database management systems including Service Packs and Cumulative Updates to the database management systems.	7,907	8,897	8,897	9,346
Installing and configuring of mainframe software, troubleshooting issues and performing ongoing maintenance, including Service Packs and Cumulative Updates.	4,613	3,607	3,607	3,789
Provide application support and services throughout the life of an application/service. In this capacity, provide ongoing system administration and maintenance. Includes request to retire the application/service when it meets the end of its useful life. Review service/application code, coding techniques, program design and interaction with data sources to improve application/service performance and efficiency. Design and implement system security.	12,152	14,720	14,720	15,462

Projected Outcomes (Privacy Security & Disclosure)

(in Hours)

	Workload Measure	2012-2013	2013-14	2014-15	2015-16
ISOU - growth	Information Security Oversight activities	9,000	9,000	10,500	10,500
IDRT - growth	Intrusion incident monitoring and response (IDRT) activities	8,400	8,400	10,500	10,500
CMU - growth	Application assessment and certification activities	4,200	4,200	6,300	6,300
CMU pen testing - new workload	Penetration testing activities	N/A	N/A	2,100	2,100
Internal Investigations - new workload 13/14 and growth	ISAU Internal Investigations activities	6,300	6,300	10,500	10,500

Analysis of Problem

WSS - new workload	Create/conduct routine physical access audits to identify badge or access misuse	N/A	N/A	200	200
	Provide support, assistance to ISAU Investigators	N/A	N/A	200	300
	Review systems and system reports to: identify technical issues that would have been unreported, conduct trend analysis and predictive modeling, identify all other items, issues, events that would have been unreported	N/A	N/A	1,600	1,600
Data Security Tool - new workload	Install, configure, support and maintain a new Data Security tool	N/A	N/A	N/A	2,100

F. Analysis of All Feasible Alternatives

Alternative #1: Approve full request of \$2.6 million and seven positions in 2014/15 and \$1.2 million and nine positions in 2015/16.

This will allow FTB to meet increased workload demands for securing FTB's critical assets and ensuring confidentiality and privacy of taxpayer information. The funding will also allow FTB to procure and install a Data Security Monitoring and Auditing system that will provide a comprehensive data audit and protection suite for preventing data theft, strengthening data privacy, and managing user access rights.

Alternative #2: Approve only the funding for the seven positions in 2014/15.

FTB will continue to use a manual, labor-intensive process to analyze logs on reported incidents. With this process, if a data breach incident occurs, FTB might not have sufficient information to conduct a complete and accurate forensic analysis. The manual process does not provide consistent verifiable audit trails in compliance with federal statutes and regulations, and does not offer an enterprise tool to provide data baseline standards and enforcement. Without remediation of the current situation, FTB runs the risk of a data breach that could expose confidential records and could be costly for the state to rectify.

Alternative #3: Approve only the funding for the Data Security Monitoring and Auditing system and two positions in 2015/16.

This alternative does not allow FTB to address the increased workload demands for securing FTB's critical assets and ensuring confidentiality and privacy of taxpayer information. It is extremely important for FTB to protect taxpayer information to maintain public trust and to encourage self compliance with tax laws.

Alternative #4: Do not approve the request.

By not approving this request FTB will run the risk of data breaches, which could result in costly threats and compromise the confidential data we are entrusted. FTB will not be in compliance with departmental policy, as well as federal statutes and regulations.

G. Implementation Plan

- June 2014 – 607 documents to establish seven positions are prepared and approved by the FTB Budget Officer and forwarded to the Department of Finance.
- June 2014 – DOF notifies FTB of position approval.
- July 1, 2014 – Funding is provided and positions are established. FTB begins hiring.
- October 2014 – Award procurement of data security tool.
- November - December 2014 – Installation and configuration of data security tool.
- November - December 2014 – Data security tool training.
- May 2015 – Install and configure data security tool in production environment.
- June 2015 – 607 documents to establish two positions for BY+1 are prepared and approved by the FTB Budget Officer and forwarded to the Department of Finance.
- June 2015 – DOF notifies FTB of position approval.
- July 2015 – Implement data security tool into operation.
- July 1, 2015 – Positions are established. FTB begins hiring.

Analysis of Problem

Supplemental Information

None Facility/Capital Costs Equipment Contracts Other One-Time Costs

- Facility Cost to build new stations in security suite.
- Contract Cost for solution provider to support data security system.
- One-Time Costs for Hardware/Software data security system.

H. Recommendation

Alternative #1 is recommended. This proposal will reduce the risk of a data breach and will allow FTB to meet current security workload demands. FTB will be in compliance with departmental policy, as well as Federal statutes and regulations.

TECHNOLOGY SERVICES DIVISION
 INFRASTRUCTURE SERVICES BUREAU
 PUC 772
 JULY 2015 PROPOSED

DATABASE SUPPORT SECTION S
 PUC 772
 DPM III 1393
 002 Susanna P Chung
 (34/1)

Database Architecture & Project Management
 (1) SSS III 1367

DB2 & ADABAS & ORACLE DATABASE SUPPORT U
 (1) SSS III (Sup) 1559
 002 Harry J. Ezray
 (17)

SQL SERVER & SYBASE DATABASE SUPPORT U
 (1) SSS III (Sup) 1559
 004 Mark D Cooley
 (15)

(1) DPM III 1393
 990 Mahmood Sitarian
 (1)

ADABAS & DB2 z/OS Database Support
 (5) SSS III 1367
 (10) SSS II 1373
 (1) SSS II 1373

SQL Server Database Support
 (1) SSSIII 1367
 (6) SSS II 1373
 (1) SSS I 1587

SYBASE Database Support
 (2) SSSIII 1367
 (3) SSS II 1373
 (1) SSS I 1587

Total Positions: 34

Administration Services Division
Privacy, Security & Disclosure Bureau
PUC 184
Proposed

36 Permanent FT filled
3 Vacant
39 Permanent Positions Total
0 Permanent Intermittent Positions
1 Retired Annuitant
0 Student Assistant
0 Seasonal Clerk
0 Temp Help
40 Positions Total

Privacy, Security & Disclosure Bureau **B**
PUC 184
CEA II 7500
001 Denise Mellor

Privacy & Security Analyst (1)
SSA 5157
001 Maria C. Arriaga

Worksite Security Section **S**
184 (9)
ADM II 4357
002 Rebecca L. Cartwright

Information Security and Oversight Section **S**
184 (32)
DPM III (Sup) 1393
002 Janine Scheidegger

Security Operations **U**
(3)
AD I 4358
001 Cordis R. Clayton

Security and Emergen Services **U**
(2)
AGPA 5393
003 Uschi U. Turner
AOS 5334
002 Patricia I. Kemp

Worksite Security Technology **U**
(2)
SSS II (Tech) 1373
008 Randall J. Garrett
ASSS (Tech) 1585
002 Jared R. Ladd
AGPA
XXX BCP 14/15

Internal Investigations and Info Sec Audit Unit **U**
(17)
SSS III (Sup) 1559
002 Lori Sanfillipo

Information Security Oversight Unit **U**
(4)
SSS III (Tech) 1367
003 Christopher W. Rushkin
SSS II (Tech) 1373
007 Anthony Greenwell
019 Timothy W. Grimmatt
010 Joseph Impinna
XXX BCP 14/15 Request

Info Security Oversight Operations **U**
(10)
SSS III (Sup) 1559
001 Quon F. Chen

AGPA 5393
001 Gregorio A. Wesley-Smith
004 Harold Leon Moore

Internal Investigations and Info Sec Audit Team
(9)
Sr. ISA (Sup) 1340
001 Jennifer L. Alekman

Info Security Audit and Employee Investigations Technical
SSS III (Tech) 1367
002 Stephen P. Norton
005 Jackquiline K. Davey
017 Wendy A. Williams
Staff PA 1581
002 Kou Vang
Technical Audit
SSS III (RA) 1559
990 Darlene L. Sedlacek
SSS II (Tech) 1373
015 Vacant
Staff ISA (Spec) 1312
004 Ngan N. Dang

Compliance Monitoring Team
Application:
SSS III (Tech) 1367
004 Cannie K. Hung, **Lead**
SSS II (Spec) 1373
XXX BCP 14/15
XXX BCP 14/15
SSS I (Spec) 1587
XXX Vacant
System:
SSS II (Tech) 1373
013 Jon P. McLinn
016 Kris A. Olson
006 Ling Luo

Intrusion Detection Team
SSS II (Tech) 1373
005 Tami L. McGee
014 Edwin Y. Gonzales
018 Richard G. Busman
XXX BCP 14/15
XXX BCP 15/16
SSS I (Spec) 1587
005 Jane D. Haxton

Internal Investigation
Staff ISA (Spec) 1312
002 Nancy S. Dablin (Lead)
003 Robert S. Mayorga
005 Heather Youngberg
XXX BCP 14/15
SSA
XXX BCP 14/15

Info Security Audit
Assoc. ISA 1470
011 Lorena E. Schubert
017 Georgetta F. Hansen
XXX Vacant
XXX Vacant