

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

Fiscal Year 2014-15	BCP No.	Org. Code 0860	Department State Board of Equalization	Priority No.
Program Administration Department			Element	Component N/A

Proposal Title  
 INTRUSION DETECTION/INTRUSION PREVENTION SYSTEM – INFORMATION SECURITY

Proposal Summary  
 The Board of Equalization (BOE) requests \$852,000 (\$556,000 General Fund (GF), \$296,000 Reimbursements) and 6.0 permanent positions in fiscal year (FY) 2014-15 and \$759,000 (\$496,000 GF, \$263,000 Reimbursements) in FY 2015-16 and ongoing for the BOE to administer, maintain and inspect the network security solutions that comply with the Internal Revenue Service (IRS) Publication (Pub) 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*. Compliance with IRS guidelines is necessary to ensure the BOE's ability to continue to utilize IRS tax information which is critical to the collection of estimated \$3-5 million revenue annually.

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 No	Code Section(s) to be Added/Amended/Repealed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.      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.*

Budget Officer	Date	Chief, Financial Management Division	Date
Deputy Director, Administration	Date	Executive Director	Date

**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

**STATE BOARD OF EQUALIZATION**  
**Administration Department**  
**Intrusion Detection/Intrusion Prevention System – Information Security**  
**Fiscal Year 2014-15**

**A. Proposal Summary**

The Board of Equalization (BOE) requests \$852,000 (\$556,000 General Fund (GF), \$296,000 Reimbursements) and 6.0 permanent positions in fiscal year (FY) 2014-15 and \$759,000 (\$496,000 GF, \$263,000 Reimbursements) in FY 2015-16 and ongoing for the BOE to administer, maintain and inspect the network security solutions that comply with the Internal Revenue Service (IRS) Publication (Pub) 1075, Tax Information Security Guidelines for Federal, State and Local Agencies. Compliance with IRS guidelines is necessary to ensure the BOE's ability to continue to utilize IRS tax information which is critical to the collection of estimated \$3-5 million revenue annually.

The BOE is required to install an Intrusion Detection System and an Intrusion Prevention System (IDS/IPS) in order to comply with IRS Pub 1075. In addition, the IRS is also requiring employees working in the BOE's field offices to wear identification badges. The BOE is requesting 6.0 positions to administer and maintain the network security solutions, perform internal Federal Tax Information (FTI) safeguard inspections of 42 business units (27 field offices, 12 headquarter units, and 3 OTech backup server locations), and maintain security badging for the 27 field offices.

**B. Background/History**

Historically, the bulk of the BOE's corporate taxpayer data has been maintained at the OTech Data Center. In addition, public facing applications, such as e-File, are housed at OTech. Due to rising costs for OTech services, the BOE has been providing internal server space for some FTI and other confidential data. Periodically, the IRS reviews the BOE's safeguards in place to ensure compliance with IRS Pub 1075 to protect FTI and the latest of those audits has determined that the BOE's existing safeguards require enhancements to be fully compliant. The IDS/IPS will monitor all network entry and exit points looking for specific activities that could indicate an attack or malicious activity which could threaten the security of the tax data.

The BOE is required to purchase and install an IDS/IPS and must configure it to specifically address each host that receives, transmits, processes, and stores FTI. This includes documenting the baseline IDS/IPS settings and any deviations necessary to maintain normal business operations. This documentation must include a listing of suspicious events that the IDS/IPS is monitoring and preventing. All this generated documentation needs to be monitored and checked for false positives, therefore, the BOE needs to augment personnel levels to continuously support, audit and monitor the network security solutions and safeguard practices.

IRS Pub 1075 requires the BOE to perform internal inspections (audits) to evaluate the effectiveness of controls over FTI, including an IPS/IDS solution. This requirement prescribes that BOE field offices must be reviewed within a 3-year cycle, and Headquarters (HQ) office facilities housing FTI and the agency computer facility (OTech) reviewed within an 18-month cycle.

In addition, the IRS is also requiring employees working in the BOE's 27 field offices to wear identification badges as a second barrier to protect FTI.

**C. State Level Considerations**

The BOE collects taxes and fees that provide approximately 34 percent of the annual revenue for state government and essential funding for counties, cities, and special districts. In fiscal year 2010-11, the BOE-administered taxes and fees produced \$53.7 billion for education, public safety, transportation, housing, health services, social services, and natural resource management. The BOE administers the state's sales

and use, fuel, alcohol, tobacco, and other taxes and collects fees that fund specific state programs. More than one million businesses are registered with the agency.

FTI directly assists the BOE in collecting \$3-5 million in annual revenue. If FTI is not protected up to the requirements of the IRS the BOE risks access to FTI to be eliminated. This would result in loss of revenue currently being generated from FTI. This proposal will ensure that the BOE addresses the mandates from the IRS to comply with IRS Pub 1075. To achieve this we will need highly skilled information security analyst staff with the technical ability to maintain and administer our network security solutions.

#### **D. Justification**

The BOE must comply with the IRS Pub 1075 in order to use FTI provided by the IRS, and because the BOE has FTI in-house and must purchase and install the IDS/IPS, staff will be needed to maintain the systems, review the output and inspect safeguards (controls). An IDS/IPS is a device similar to a burglar alarm that monitors exit points of a building and alerts a monitoring company that can contact the Police or Fire Department depending on the alarm triggered. An IDS/IPS monitors all access points of a network or system looking for malicious activities or policy violations and produces reports to one or many management stations. In addition, IDS/IPS can be used for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDS/IPS has become a necessary addition to the security infrastructure of nearly every organization. The monitoring portion of the IDS/IPS records information related to observed events, notifies security administrators of important observed events and produces reports. IDS/IPS also responds to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content. Attacks can occur from external sources as well as internal sources.

Maintaining, monitoring, and auditing these systems will require full time staff to respond to events that change the system to prevent attacks as well as to monitor and review event logs to determine the source of attacks and any resulting damage. The BOE needs to have highly skilled personnel to support and maintain the network security enhancements. The BOE requires 1.0 permanent full-time Staff Information Systems Analyst for the Information Security Office, 1.0 permanent full-time Senior Information Systems Analyst and 1.0 permanent full-time Staff Information Systems Analyst for the Technology Services Division (TSD) and 2.0 permanent full-time Business Taxes Specialist II positions to perform FTI safeguard inspections to meet IRS Pub 1075 requirements. These specialists will perform internal audits designed to provide an independent and objective evaluation of FTI safeguard policies, procedures, internal controls, record retention practices, access control, and network security and configuration settings to comply with IRS requirements based on National Institute of Standards and Technology special publication 800-53.

The BOE is also requesting a 1.0 permanent full-time Associate Governmental Program Analyst for the Physical Security Section to administer all badge/ID card related tasks and requests for 4000+ employees in the BOE Headquarters (HQ), annex, and field offices. The associate analyst will be responsible for the following tasks:

- Manage, coordinate, and oversee all ID card/ badge related activities statewide
- Continuous analysis of ID card issuance process and assessment of its effectiveness
- Submit regular status reports and recommendations to management to improve operational process
- Identify and address recurring issues or complaints field office staff may attempt to communicate
- Solve arising ID card related issues effectively while maintaining a high level of courtesy and customer service etiquette
- Function as liaison to the BOE field offices and address ID card related inquires
- Ensure that ID card related processes remain in compliance with established policies and procedures, of State Law, confidentiality agreements, as well as internal protocol
- Procurement of supplies required for the creation, issuance, management, and distribution of ID cards
- Manage, update, and maintain an electronic database capturing ID card related information

- Implement any changes to the process mandated by management or new laws in a swift and effective manner that will not obstruct or delay business continuation
- Find creative and innovative ways to implement new technology, procedures, and processes

#### **E. Outcomes and Accountability**

This proposal will bring the BOE in compliance with the IRS requirements by enhancing access control, network and physical security and internal inspections. Network security enhancements will include an active IDS/IPS aiding the BOE in safeguarding network assets, while the Security Incident Event Management log monitoring will allow the BOE to determine what types of events occurred on the network, such as data loss, denial of service, and other serious threats.

#### **F. Analysis of All Feasible Alternatives**

**Alternative 1 – Approve 6.0 permanent positions to administer the network security solutions, internal inspections and security badging for field offices.**

##### **Pros:**

- Preserve \$3-5 million in revenue annually by maintaining access to FTI
- Addresses mandate of IRS Pub 1075 compliance
- Grants dedicated staff to provide daily operational support of the IDS/IPS to enhance security and provide improved protection of taxpayer information
- Allows the BOE to provide technical training and mentoring to junior level engineers/technicians by hiring highly skilled and trained staff
- Devotes more time to supporting current and upcoming network security enhancements
- Avoids contracting with private companies for ad hoc support by having dedicated staff for network security
- Provides required second barrier to protect FTI in field offices

##### **Cons:**

- Requires budget augmentation

**Alternative 2 – Approve 6.0 three year limited-term positions to provide needed support.**

##### **Pros:**

- Preserve \$3-5 million in revenue annually by maintaining access to FTI
- Temporarily addresses mandate of IRS Pub 1075 compliance
- Temporarily dedicates staff to provide daily operational support of the IDS/IPS to enhance security and provide improved protection of tax payer's information
- Hiring highly skilled and trained staff allows the BOE to provide technical training and mentoring to junior level engineers/technicians
- Specialist will be able to devote more time to supporting current and upcoming network security enhancements
- Avoids contracting with private companies for ad hoc support by having dedicated staff for network security
- Provides required second barrier to protect FTI in field offices

##### **Cons:**

- Requires budget augmentation
- Risks not being able to fill positions due to the limited term nature
- Risks high turnover in position requiring increased costs to train new employees
- Could leave systems unmonitored due to vacancies

### Alternative 3 – Contract with OTech to provide the IDS/IPS service

**Pros:**

- Preserve \$3-5 million in revenue annually by maintaining access to FTI
- Systems would already be protected by OTech Security Infrastructure

**Cons:**

- Costs for services at OTech would be near \$1 million greater than providing the service In-house (Based on 5 years cost estimate comparisons)
- Significant cost increases by having OTech provide services year over year
- Could result in delays in responding to incidents due to potential questions of responsibility
- Does not protect the in-house assets of the BOE
- Does not address the need to provide staff badging, and badge management

### Alternative 4 – Do not approve this request

**Pros:**

- Does not require a budget augmentation and would require a larger budget augmentation for the BOE

**Cons:**

- Risk of loss of use of FTI data and the \$3-5 million in annual revenue associated with its use
- Slower implementation of various strategic and mandated network security initiatives
- Without staff the BOE will be in jeopardy of not complying with IRS Pub 1075 as mandated for access to FTI
- Additional workload for network security work will impact current staffing levels and workloads which will result in lack of resources for other projects and day to day operations
- Existing staff may need to take on duties not in their job descriptions, necessitating position changes and potentially higher salary ranges, costing more in the long term
- Additional cost of training for current staff will be necessary

## G. Implementation Plan

Enhance network security

- July 2014 – Hire staff
- August 2014 – Train staff by vendor
- September 2014 – Verify IRS Pub 1075 compliance
- Ongoing support of the network security enhancements

Enhance internal inspections

- July 2014 – Hire staff
- August 2014 – Train staff
- Ongoing performance of FTI safeguards internal inspections

Expand Security Badging

- July 2014 – Hire staff
- August 2014 – Train staff
- Ongoing support for security badging

## H. Supplemental Information (Check box(es) below and provide additional descriptions.)

- None     Facility/Capital Costs     Equipment     Contracts     Other

**I. Recommendation**

**Alternative one is recommended.**

Approve 6.0 permanent positions to support IRS mandated enhancement to the network and physical security, and perform internal inspections.

DRAFT

**Workload Detail for Intrusion Detection/Intrusion Prevention System – Information Security**

**INFORMATION SECURITY OFFICE (ISO)**

**1.0 Staff Information Systems Analyst**

The ISO has been tasked with providing system automated log review and analysis, resulting in a permanent workload increase for existing staff. Position would be responsible for conducting scans, as well as review of the system generated audit logs. Following review and analysis, the position is required to notify ISO and TSD management of issues, included indications of ongoing or imminent risk, vulnerabilities or threats to the BOE network. As required, the position would be the lead in creating reports on a daily basis indicating the overall trends and patterns of network activity.

<b>Workload Detail</b>				
<b>Classification:</b> Staff Information Systems Analyst	<b>Time Measure</b>		<b>On-going Activities</b>	
<b>Activity</b>	<b>M=Minutes H = Hours</b>	<b>Time Per Occurrence</b>	<b>Occurrences Per Year</b>	<b>Total Hours</b>
Analysis of Security Incident Event Management activity logs.	H			600
Analysis of other security related systems logs.	H			360
Development of security risk trend analysis matrices.	H			360
Coordinate development of network remediation plans based on analysis of events and trends.	H			180
Assist in the planning, selection, and testing of security software/hardware products.	H			100
Assist with vulnerability scans.	H			100
Create edit and generate reports based on analysis.	H			100
Total 1800 hours				1800
Total 1 Positions Requested (1,800 Hours/Position)				<b>1.0</b>

**PHYSICAL SECURITY SECTION (PSS)**

**1.0 Associate Governmental Program Analyst**

The PSS has been tasked with providing field office support, resulting in a permanent workload increase for existing staff. Due to an IRS mandate, all field office staff must be issued an ID card. Consequently, the PSS must issue ID cards statewide to every new employee, as well as maintain current workload at the BOE HQ. The ongoing badge maintenance workload, such as name change requests, profile updates, and replacement ID cards, will increase due to the number of the additional staff.

<b>Workload Detail</b>				
<b>Classification:</b> Associate Governmental Program Analyst	<b>Time Measure</b>		<b>On-going Activities</b>	
<b>Activity</b>	<b>M=Minutes H = Hours</b>	<b>Time Per Occurrence</b>	<b>Occurrences Per Year</b>	<b>Total Hours</b>
Receive request and review for completion and accuracy, correspond with requestor as necessary.	H			180
Obtain and edit corresponding employee photograph for ID card; follow-up with requestor as necessary.	H			180
Create employee profile in the security system and upload photograph into database.	H			360
Print ID card and prepare corresponding paperwork for distribution with card.	H			360
Ship ID card, instructions, and BOE 508A <i>Employee Badge or ID Card Request</i> to district administrator, send email notification of shipment.	H			180
Track, receive, review, and file returned paperwork; update security system and tracking log.	H			270
Inventory control, procurement and distribution of ID card supplies to all field offices.	H			180
Correspond with field offices, vendors, and Acquisitions regarding supplies.	H			90
<b>Total hours</b>				<b>1800</b>
<b>Total Positions Requested</b>				<b>1.0</b>

**TECHNOLOGY SERVICES DEPARTMENT (TSD)**

**1.0 Senior Information Systems Analyst and 1.0 Staff Information Systems Analyst**

The TSD has been tasked with providing IDS/IPS support, resulting in a permanent workload increase for existing staff. Due to an IRS mandate, the BOE is required to implement a new IDS/IPS which will monitor the network as part of safeguarding the BOE’s assets. This workload increase on existing staff must be augmented to ensure proper system oversight, to include maintaining timely analysis of system generated alerts, mitigation of detected threats, and routine system maintenance.

<b>Workload Detail</b>				
<b>Classification:</b> Senior Information Systems Analyst	<b>Time Measure</b>		<b>On-going Activities</b>	
<b>Activity</b>	<b>M=Minutes H = Hours</b>	<b>Time Per Occurrence</b>	<b>Occurrences Per Year</b>	<b>Total Hours</b>
Provide daily operational support of the two mandated network Intrusion Detection/ Intrusion Prevention (IDS/IPS).	H			720
Troubleshoot network problems, outages, hacking/denial of service attempts, and security alerts.	H			720
Monitoring IDS/IPS logs and checking for false positives. Providing de-bugging/troubleshooting, optimization and security support.	H			90
Maintain network documentation, network drawings, and change management forms.	H			90
Provide technical training and mentoring to junior level engineers/technicians.	H			90
Consult with customers regarding network performance problems, ideas for design improvements.	H			90
Total hours				1800
Total Positions Requested				<b>1.0</b>

<b>Workload Detail</b>				
<b>Classification:</b> Staff Information Systems Analyst	<b>Time Measure</b>		<b>On-going Activities</b>	
<b>Activity</b>	<b>M=Minutes H = Hours</b>	<b>Time Per Occurrence</b>	<b>Occurrences Per Year</b>	<b>Total Hours</b>
Provide daily operational support of the two mandated network Intrusion Detection/ Intrusion Prevention (IDS/IPS).	H			740
Troubleshoot network problems, outages, hacking/denial of service attempts, and security alerts.	H			720
Monitoring IDS/IPS logs and checking for false positives. Providing de-bugging/troubleshooting and security support.	H			160
Maintain network documentation, network drawings, and change management forms.	H			90
Consult with customers regarding network performance problems.	H			90
Total hours				1800
Total Positions Requested				<b>1.0</b>

**INTERNAL AUDIT DIVISION (IAD)**

**2.0 Business Taxes Specialist II**

The IAD has been tasked with performing FTI safeguard audits, resulting in a permanent workload increase for existing staff. Due to the IRS Pub 1075 mandate, all field office, HQ and agency computer facilities housing FTI must be inspected on either a 3-year or 18-month cycle. Consequently, the IAD must perform on average 17 FTI safeguard audits every year.

<b>Workload Detail</b>				
<b>Classification:</b> Business Taxes Specialist II	<b>Time Measure</b>		<b>On-going Activities</b>	
<b>Activity</b>	<b>M=Minutes H = Hours</b>	<b>Time Per Occurrence</b>	<b>Occurrences Per Year</b>	<b>Total Hours</b>
<u>Initiation and Planning</u> – Research and background, prepare risk and control matrix, document data and records process flow, prepare planning memo, entrance conference, preliminary survey, prepare audit program.	H			900
<u>Execution/Fieldwork</u> – Facilitate meetings, interview staff, observations and inspections, benchmarking, evaluation of internal controls, analytical reviews, physical inspections, network configuration testing, access control inspections, prepare summary of findings.	H			1440
<u>Reporting</u> – Review audit findings with auditee, prepare draft report, issue and evaluate corrective action plan responses, prepare and issue final report.	H			900
<u>Closing &amp; Follow-Up</u> – Issue destruction of records memo (if necessary), clean-up and file audit working papers, perform follow-up evaluation (6 months post audit) to ensure corrective actions effectively mitigate identified risk.	H			360
Total hours				3600
Total Positions Requested				<b>2.0</b>

**Fiscal Summary**  
(Dollars in thousands)

BCP No. <b>4</b>	Proposal Title <b>Intrusion Detection/Intrusion Prevention System</b>	Program			
<b>Personal Services</b>		<b>Positions</b>	<b>Dollars</b>		
		<b>CY</b>	<b>BY</b>		
		<b>BY + 1</b>	<b>CY</b>		
		<b>BY</b>	<b>BY + 1</b>		
Total Salaries and Wages <sup>1</sup>		6.0	6.0		
Total Staff Benefits <sup>2</sup>					
<b>Distributed Administration</b>					
<b>Total Personal Services</b>		6.0	6.0		
<b>Operating Expenses and Equipment</b>					
General Expense			\$91		
Distributed Administration					
Printing					
Communications			\$14		
Postage					
Travel-In State					
Travel-Out of State					
Training			\$5		
Facilities Operations			\$68		
Utilities			\$1		
Consulting & Professional Services: Interdepartmental <sup>3</sup>					
Consulting & Professional Services: External <sup>3</sup>					
Data Center Services			\$15		
Information Technology Equipment <sup>3</sup>			\$29		
Other/Special Items of Expense: <sup>4</sup>					
<b>Total Operating Expenses and Equipment</b>			\$223		
<b>Total State Operations Expenditures</b>			\$852		
			\$759		
<b>Fund Source</b>	<b>Item Number</b>				
	<b>Org</b>	<b>Ref</b>	<b>Fund</b>		
General Fund	0860	001	0001	\$556	\$496
Special Funds <sup>5</sup>					
Federal Funds					
Other Funds (Specify)					
Reimbursements	0860	001	0995	\$296	\$263
<b>Total Local Assistance Expenditures</b>					
<b>Fund Source</b>	<b>Item Number</b>				
	<b>Org</b>	<b>Ref</b>	<b>Fund</b>		
General Fund					
Special Funds <sup>5</sup>					
Federal Funds					
Other Funds (Specify)					
Reimbursements					
<b>Grand Total, State Operations and Local Assistance</b>				\$852	\$759

1 Itemize positions by classification on the Personal Services Detail worksheet.

2 Provide benefit detail on the Personal Services Detail worksheet.

3 Provide list on the Supplemental Information worksheet.

4 Other/Special Items of Expense must be listed individually. Refer to the Uniform Codes Manual for a list of standard titles.

5 Attach a Fund Condition Statement that reflects special fund or bond fund expenditures (or revenue) as proposed.

## Personal Services Detail

(Whole dollars)

BCP No.	Proposal Title <b>Intrusion Detection/Intrusion Prevention System</b>						
<b>Salaries and Wages Detail</b>							
Classification <sup>1 2</sup>	Positions			Salary Range	Dollars		
	CY	BY	BY + 1		CY	BY	BY + 1
<b>Administration Department</b>							
<b>ISO</b>					\$0	\$0	\$0
Staff Information Systems Analyst		1.0	1.0	\$70,356	\$0	\$70,356	\$70,356
<b>PSS</b>							
Associate Governmental Program Analyst		1.0	1.0	\$59,448	\$0	\$59,448	\$59,448
					\$0	\$0	\$0
<b>Technology Services Department</b>							
Senior Information Systems Analyst		1.0	1.0	\$77,364	\$0	\$77,364	\$77,364
Staff Information Systems Analyst		1.0	1.0	\$70,356	\$0	\$70,356	\$70,356
					\$0	\$0	\$0
<b>Executive Department</b>							
<b>IAD</b>							
Business Taxes Specialist II		2.0	2.0	\$77,400	\$0	\$154,800	\$154,800
					\$0	\$0	\$0
					\$0	\$0	\$0
					\$0	\$0	\$0
Blanket Funds:							
Overtime					0	0	0
Temporary Help	0.0	0.0	0.0		0	0	0
<b>Total Salaries and Wages <sup>3</sup></b>	0.0	6.0	6.0		\$0	\$432,324	\$432,324
<b>Staff Benefits Detail</b>					<b>CY</b>	<b>BY</b>	<b>BY + 1</b>
OASDI						33,073	33,073
Health/Dental/Vision Insurance						68,692	68,692
Retirement						88,639	88,639
Miscellaneous							
Workers' Compensation						3,934	3,934
Industrial Disability Leave						415	415
Non-Industrial Disability Leave						177	177
Unemployment Insurance						346	346
Other:						1,297	1,297
<b>Total Staff Benefits <sup>3</sup></b>					\$0	\$196,573	\$196,573
<b>Grand Total, Personal Services</b>					<b>\$0</b>	<b>\$628,897</b>	<b>\$628,897</b>

<sup>1</sup> Use standard abbreviations per the Salaries and Wages Supplement. Show any effective date or limited-term expiration date in parentheses if the position is not proposed for a full year or is not permanent, e.g. (exp 6-30-13) or (eff 1-1-13)

**Note: Information provided should appear in the same format as it would on the Changes in Authorized Positions.**

<sup>2</sup> If multiple programs require positions, please include a subheading under the classification section to identify positions by program/element.

<sup>3</sup> Totals must be rounded to the nearest thousand dollars before posting to the Fiscal Summary.