



The Council of State Governments
Sharing capitol ideas.

2011 Innovations Awards Application

DEADLINE: MARCH 28, 2011

ID # (assigned by CSG): 2011- _____

Please provide the following information, adding space as necessary:

State: California

Assign Program Category (applicant): Government Operations and Technology- Information Systems

1. **Program Name:** E-Commerce Portal Infrastructure (EPI)
2. **Administering Agency:** Franchise Tax Board
3. **Contact Person (Name and Title):** Cathy Cleek, Chief Information Officer
4. **Address:** PO Box 1468 MS A290, Sacramento, CA 95812-1468
5. **Telephone Number:** 916-845-3310
6. **FAX Number:** 916-845-9589
7. **E-mail Address:** Cathy.Cleek@ftb.ca.gov
8. **Web site Address:** <http://www.ftb.ca.gov>
9. **Please provide a two-sentence description of the program.**

Californians file more than 17 million personal and business state income tax returns with the State of California Franchise Tax Board (FTB) each year, generating more than \$60 billion for the state's General Fund. The increased use of E-Commerce (ECOM) applications to manage tax filing and collection activities resulted in the E-Commerce Portal Infrastructure project (EPI) to address network deficiencies, such as availability, manageability and security, while providing a scalable network infrastructure capable of supporting current and future E-Commerce applications.

10. **How long has this program been operational (month and year)? Note: the program must be between 9 months and 5 years old on March 28, 2011 to be considered.**

November 2009

11. **Why was the program created? What problem[s] or issue[s] was it designed to address?**

The FTB network was originally designed to support mainframe “green-screen” applications to process and record taxpayer information in a closed environment without Internet access. In the mid 1990s, FTB started providing E-Commerce services as public acceptance and demand grew. FTB leveraged the Internet to enhance tax-collection activities and added an E-Commerce network to the existing Demilitarized Zone (DMZ) to support a growing web server farm and to provide secure internal access to the Internet. The Internet and ECOM applications have grown to become FTB’s main method of conducting business. Because the vast majority of the department’s tax returns and payments are now received electronically, the department’s ECOM applications must remain available or the state can lose millions of dollars in revenue. In addition, FTB has millions of confidential tax records that must be kept protected. As FTB deployed new applications, the DMZ increased in size, complexity and risk exposure.

The risks FTB faced before the EPI Project are summed up in four main categories: Availability, Security, Scalability, and Manageability:

1. **Availability** - The infrastructure contained many single points of failure that jeopardized FTB’s ability to provide an uninterrupted ECOM environment to its internal and external customers. Many of the devices that made up FTB’s infrastructure were “single points of failure.” Taking one of these devices down for service was problematic because it also took down the entire infrastructure. Staff normally performed maintenance during scheduled maintenance windows (off hours), but this was not always possible when failures occurred. FTB also had a single Internet connection, making it extremely vulnerable to physical threats and natural disasters.
2. **Security** – FTB’s Intrusion Detection System (IDS) was reactive and was unable to block malicious attacks. Analyzing IDS data required manual diagnoses by local administrators so security responses were often slow to block threats to FTB’s confidential taxpayer data and/or network. FTB could not prevent other types of attacks, such as “zero-day” and “denial of service” attacks because the systems could not block these threats. FTB’s applications were also at risk because the department did not have internal firewalls to prevent a malicious employee from attacking systems. Also, network traffic often exceeded the capacity of the IDS resulting in that traffic not being inspected.
3. **Scalability** – The existing infrastructure limited FTB’s ability to add new applications to the DMZ. For each new application that was added to the existing environment, new hardware/software was required, which resulted in a lengthy procurement process. FTB’s ability to support its external customers was at risk. Due to frequent changes in tax law and new programs, it was difficult for FTB to implement them in a timely manner.
4. **Manageability** – FTB had no centralized management tool for network devices, making support difficult. To perform software upgrades, network engineers were required to address each device on an individual basis, often resulting in downtime. Due to dissimilar devices and software versions, it was difficult to maintain standardized configurations.

12. Describe the specific activities and operations of the program in chronological order.

Task or Activity	Begin Date		Completion Date	
	Target	Actual	Target	Actual
Project Start, Department of Finance approval	1/16/07	1/17/07	1/16/07	1/17/07
Develop and release competitive bid solicitation documents for California Multiple Awards Schedule and competitive bid acquisitions.	12/03/07	10/30/07	2/28/08	12/21/07
Award Procurement Hardware/Software Agreements	4/16/08	12/28/07	4/16/08	12/28/07
Received Hardware/Software	6/16/08	1/28/08	6/16/08	12/15/08
Configuration of Infrastructure Components	10/01/08	7/1/08	04/30/09	04/30/09

Develop Testing and Migration Plans	10/01/08	2/04/08	1/30/09	04/30/09
Move servers and applications from existing DMZ to new EPI network. Implement testing and migration plans.	5/01/09	04/30/09	11/02/09	11/19/09
Prepare Post Implementation Evaluation Report	6/01/10	09/01/10	11/02/10	01/31/11

13. Why is the program a new and creative approach or method?

FTB was the first organization in the state to implement an ECOM infrastructure of this magnitude. Innovations include:

- This environment is highly scalable due to the extensive use of virtual technology which allows FTB to add new environments as needed.
- It is highly secure and self-healing due to the use of Intrusion Detection and Prevention System (IDPS) and Distributed Denial-of-Service (DDoS) guard, which will automatically respond and block malicious and denial-of-service attacks.
- System management has been improved by the capability to administer all devices and perform troubleshooting from centralized management tools, which allows staff to perform routine maintenance and system software upgrades without affecting customers.

14. What were the program’s start-up costs? (Provide details about specific purchases for this program, staffing needs and other financial expenditures, as well as existing materials, technology and staff already in place.)

Total One-time IT Cost: \$5,795,863:

Departmental State Staff Redirection: 18.9 Personnel Years (PYs) - \$1,850,128

Hardware Purchase - \$3,171,728 Budget Change Proposal (BCP)

- Nokia CheckPoint Firewalls
- Cisco Routers, Switches, Firewalls, Load Balancers and Analysis Modules
- Cisco Network Intrusion Detection and Prevention System (IDPS)
- Cisco Security Incident and Event Management (SIEM) system

Software Purchase - \$44,659 (BCP)

- CheckPoint Licenses
- Cisco Host IDS Software
- Cisco Software Maintenance

Telecommunications Cost - \$233,773 (BCP)

- Internet Service Provider (ISP) service
- Cabinets & Wiring

Contract Services - \$370,100 (BCP)

- Design Consultant
- Cisco Network Engineer
- Cisco Security Engineer

Training/Travel – \$125,475 (BCP)

15. What are the program’s annual operational costs?

Total Annual IT On-Going Maintenance - \$1,428,389:

Departmental State Staff Redirection: 8.6 PYs - \$894,414

Hardware Lease/Maintenance - \$355,664 (Departmental Redirection)

- Nokia CheckPoint Maintenance
- Cisco Equipment Maintenance
- Cisco IDPS and SIEM Maintenance

Software Lease/Maintenance - \$105,188 (Departmental Redirection)

- CheckPoint Licenses
- Cisco Software Maintenance

Telecommunications - \$73,123 (Departmental Redirection)

- ISP service cost

16. How is the program funded?

- Personnel Services one-time costs funded through FTB Internal Departmental redirection funds.
- Operating Expense and Equipment one-time costs were funded through a Budget Change Proposal (BCP)
- Annual IT On-Going Maintenance costs are funded through FTB Internal Departmental Redirection funds.

17. Did this program require the passage of legislation, executive order or regulations? If YES, please indicate the citation number.

No

18. What equipment, technology and software are used to operate and administer this program?

The EPI design is centered on multi-layer hierarchical network architecture, eliminating single points of failure using redundant system components such as external Internet connections, network routers and security appliances.

EPI has allowed FTB to maintain network connectivity during hardware failures and during scheduled maintenance. Central to the EPI design was the introduction of virtual technology, allowing for the deployment of new applications and services without significant network redesign or the procurement of additional system components. The ECOM Portal Infrastructure is segmented into three zones: the Internet Public Zone, the Extranet Secured Zone, and the Intranet Secure Zone:

1. **Internet Public Zone** – This zone directly interfaces FTB to the Internet and provides the first layer of defense. This zone is composed of redundant perimeter routers, distributed denial of service prevention system, intrusion prevention system appliances, firewalls, a reverse proxy system and geographically diverse connections to FTB’s Internet service provider.
2. **Extranet Secured Zone** – This zone is the second layer of defense. It is comprised of redundant Edge (separates FTB’s internal network from the DMZ) and DMZ switch blocks. The Edge switch block components consist of routers, firewalls, IDPS appliances and WAN connected district offices. A second set of firewalls are authored by a different manufacturer than the firewalls in the Internet Public Zone. This switch block serves as the main gateway for all Internet and ECOM based traffic. Additionally, it is where business partner and in-bound virtual private network connections are terminated. The DMZ switch block consists of routers, firewalls, load-balancers, IDPS and switches. This switch block is where the FTB’s front-facing ECOM servers are located.
3. **Intranet Secure Zone** – This zone protects FTB’s internal network from internal attacks. It is comprised of redundant Secured Server Farm (SSF) switch blocks. The SSF switch blocks are identical to the DMZ switch blocks.

Each switch block (Edge, DMZ and SSF) is subdivided into virtual environments that are composed of virtual network devices: routers, firewalls, IDPS, load-balancers and switches. Application-specific environments can be cloned and customized from a standard configuration without the need for additional hardware. Each switch block has the capability to scale to more than 200 virtual environments. This

capability provides FTB with the capacity needed to support all new applications that will be added to our internal and external networks.

19. To the best of your knowledge, did this program originate in your state? If YES, please indicate the innovator's name, present address, telephone number and e-mail address.

Yes. FTB Network Engineering Section, PO Box 1468, MS L232, Sacramento, CA 95812-1468,
NES@ftb.ca.gov

20. Are you aware of similar programs in other states? If YES, which ones and how does this program differ?

No

21. Has the program been fully implemented?

Yes

22. Briefly evaluate (pro and con) the program's effectiveness in addressing the defined problem[s] or issue[s]. Provide tangible examples.

Pros: The EPI project had four primary goals for the new environment: Improved Availability, Security, Scalability and Manageability. The EPI project addressed all four goals as described below:

1. Availability

- a. Prior to EPI, the network was offline up to 30 minutes per month for routine maintenance. This sounds small but these outages affected (17 to 20 million) data transactions per month between FTB, partner agencies, commercial entities and individual taxpayers. Many of these transactions, and FTB maintenance activities, are typically performed during off-peak hours. The EPI infrastructure now allows routine maintenance of all devices to occur without taking the network completely offline.
- b. Most taxpayers file during the final days of the tax filing season, which places peak demands on the EPI network peak in a two week period leading up to April 15 of each year. The EPI network can now support these yearly spikes without degradation of service.
- c. EPI has allowed FTB to maintain network connectivity during hardware failures and during scheduled maintenance.

2. Security

- a. The EPI Project has aligned FTB with the Chief Information Officer and Information Security Officer guidelines, best practices and mandates for risk management and security.
- b. Threats carried by the Internet have increased in quantity and complexity. With FTB's multilayer approach to security, we have had no loss of taxpayer data due to a cyber attack.
- c. The IDPS has resulted in the detection of more than 200 malicious attacks per month, which the system was able to automatically block. In the first six month period after implementation, the DDoS system alerted us to 187 events. Overall, our visibility of threats has significantly improved.

3. Scalability

- a. In 1994, when Personal Income Tax (PIT) e-file began, FTB received 345 returns. By 2000, FTB's PIT e-file programs processed 2.5 million of California's 15 million PIT returns. By 2010, FTB's PIT e-file nearly quadrupled in volume to a staggering 11.1 million e-file returns. As ECOM applications are used by more and more people, the EPI network will be able to support the increasing demand.
- b. New revenue and benefit programs are being added each year by the legislature. In the past, it was difficult to meet the short deadlines for instituting the new mandates, due to the amount of

time it took to physically redesign the existing ECOM network and procure additional equipment. Using virtual environment technology, EPI allows new applications to be added quickly.

4. Manageability

- a. Since February of 2009, FTB employees have been impacted by mandatory state furloughs. The EPI infrastructure has provided an infrastructure that is easily scalable, allowing new applications to be added with minimal efforts, allowing existing personnel resources to “do more with less”.
- b. FTB’s support changed from a reactive (fire-fighting) approach, to a proactive maintenance support model.
- c. With EPI, application-specific environments can be cloned and customized from a standard configuration without the need for additional hardware. This means that FTB has the capacity to easily support all new applications that will be added to our internal and external networks.

Cons:

1. The introduction of many cutting edge technologies to our environment simultaneously required FTB staff to be highly trained.
2. The cost of this technology was significant, but necessary given FTB’s obligation to protect taxpayer data and ensure the collection of revenue.

23. How has the program grown and/or changed since its inception?

Due to the scalable design and the use of virtual technology, we have added multiple new environments with minimal effort and no additional equipment.

24. What limitations or obstacles might other states expect to encounter if they attempt to adopt this program?

A similar project of this magnitude will require highly technical staff from different competencies, and a high level of teamwork from project design to implementation.

CSG reserves the right to use or publish in other CSG products the information provided in this application. If your agency objects to this policy, please advise us in a separate attachment.



The Council of State Governments
Sharing capitol ideas.

2011 Innovations Awards Application Program Categories and Subcategories

Use these as guidelines to determine the appropriate Program Category for your state's submission and list that program category on page one of this application. Choose only one.

Infrastructure and Economic Development

- Business/Commerce
- Economic Development
- Transportation

Government Operations and Technology

- Administration
- Elections
- Information Systems
- Public Information
- Revenue
- Telecommunications

Health & Human Services

- Aging
- Children & Families
- Health Services
- Housing
- Human Services

Human Resources/Education

- Education
- Labor
- Management
- Personnel
- Training and Development
- Workforce Development

Natural Resources

- Agriculture
- Energy
- Environment
- Environmental Protection
- Natural Resources
- Parks & Recreation
- Water Resources

Public Safety/Corrections

- Corrections
- Courts
- Criminal Justice
- Drugs
- Emergency Management
- Public Safety

Save in .doc or rtf. Return completed application electronically to innovations@csg.org or mail to:

CSG Innovations Awards 2011
The Council of State Governments
2760 Research Park Drive, P.O. Box 11910
Lexington, KY 40578-1910

Contact:

Nancy J. Vickers, National Program Administrator
Phone: 859.244.8105
Fax: 859.244.8001 – Attn: Innovations Awards Program
The Council of State Governments
E-mail: nvickers@csg.org

This application is also available at www.csg.org.