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

Fiscal Year	Business Unit	Department	Priority No.
2023-24	7730	Franchise Tax Board	005

Budget Request Name	Program	Subprogram
7730-005-BCP-2023-GB	6280/6290/6295	6280010/6280019/6280025

Budget Request Description
Security and Access Management

Budget Request Summary
The Franchise Tax Board (FTB) is requesting $1.8 million, $1.77 million General Fund and $35 thousand special funds, for two permanent positions, and software costs in FY 2023-24; $1.6 million, $1.57 million General Fund and $30 thousand special funds, for two permanent positions and software costs in 2024-25, FY 2025-26, and ongoing to reduce security risk by implementing a solution to add Privileged Access Management (PAM) capabilities and improve login security by integrating multi-factor authentication (MFA) into FTB's public web applications in compliance with Cal-Secure direction.

Requires Legislation	Code Section(s) to be Added/Amended/Repealed
☐ Yes ☒ No	

Does this BCP contain information technology (IT) components? ☒ Yes ☐ No *If yes, departmental Chief Information Officer must sign.*	Department CIO	Date

For IT requests, specify the project number, the most recent project approval document (FSR, SPR, S1BA, S2AA, S3SD, S4PRA), and the approval date.

Project No. **Project Approval Document:**

Approval Date:

If proposal affects another department, does other department concur with proposal? ☐ Yes ☐ No
Attach comments of affected department, signed and dated by the department director or designee.

Prepared By	Date	Reviewed By	Date
Department Director	**Date**	**Agency Secretary**	**Date**

Department of Finance Use Only

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

PPBA	Date submitted to the Legislature

A. Budget Request Summary

The Franchise Tax Board (FTB) is requesting $1.8 million, $1.77 million General Fund and $35 thousand special funds, for two permanent positions, and software costs in FY 2023-24; $1.6 million, $1.57 million General Fund and $30 thousand special funds, for two permanent positions and software costs in 2024-25, FY 2025-26, and ongoing to reduce security risk by implementing a solution to add Privileged Access Management (PAM) capabilities and improve login security by integrating multi-factor authentication (MFA) into FTB's public web applications in compliance with Cal-Secure direction.

B. Background/History

FTB's mission is to help taxpayers file timely and accurate tax returns, and pay the correct amount to fund services important to Californians. FTB's primary function is to administer the California Revenue and Taxation Code (R&TC), which includes collecting the proper amount of tax revenue and operating other entrusted government programs. FTB strives to serve the public by continually improving the quality of products and services and performing in a manner warranting the highest degree of public confidence with integrity, efficiency, and fairness. In FY 2021-22, FTB processed more than 22.5 million tax returns and 10 million payments, responded to more than 2.9 million telephone calls, serviced 70 million internet contacts, and collected about $190 billion in revenue, representing approximately 77 percent of California's General Fund revenue[1].

FTB has many tax and non-tax programs that directly support its mission, and information technology (IT) plays a significant role. Two areas for improvement related to IT have been identified; the first is related to system access. To maintain IT systems, higher levels of access (privileged access) are assigned to staff that are maintaining and upgrading those systems. That access is granted manually and long-term. Secondly, FTB provides taxpayers access to their account information online and we have the opportunity to strengthen access to that system. This request addresses these two security and access management technologies in need of modernization which will assist FTB's compliance with SAM 5360 Identity and Access Management and SIMM 5300 B.

System Access: Privileged Access Management (PAM):

Privileged access is a higher level of permission to make changes to a given system, application, or data. PAM is a strategy that includes policies, processes, procedures, and tools that govern how privileged access is controlled. Where appropriate, privileged access is granted to staff, vendors, systems, and applications. PAM helps FTB meet IT security compliance requirements. PAM also reduces the risk of misuse of privileged access, which in turn reduces the risk to FTB's business from the loss of confidentiality, integrity, or availability of systems, applications, and data.

Multi-Factor Authentication (MFA):

MFA is a security enhancement that requires at least two pieces of evidence from the registrant when logging into an account and is an important part of any modern authentication method. FTB uses MFA in its employee and vendor authentication but has yet to implement a method in our public web applications with external tax professionals, business representatives, and individual taxpayers. Currently, once accounts are set up, our external applications require only authentication by single factor of a user ID and password combination. This single method is non-compliant with FTB Information Security Policy 9500 Section 215; SAM (State Administrative Manual) Policy 5360, Identity and Access Management Section; Cal-Secure Strategic Plan; and IRS Publication 1075. Adding an additional method of authentication, such as a one-time passcode response where the user must use an additional channel of communication, such as a phone call or text, and reply with a generated code, would significantly improve FTB's login security.

Over the past several years FTB's Technology Services Division (TSD) has consistently been asked to implement changes and adopt new workloads through legislative change or change requests.

[1] Revenue figures based on the 2021-22 Cash Report reported in the Department of Finance's July 2022 Finance Bulletin.

At the same time, FTB must provide ongoing technical maintenance activities to ensure its systems and related infrastructure are on supported versions and contain the latest security patches so that FTB can continue to safeguard taxpayer information and provide timely return-processing services to a variety of key stakeholders (e.g., taxpayers, tax preparers). These factors have contributed to FTB's TSD struggling to fulfill the responsibility of complying with evolving security policies and standards and reducing departmental security risks and accomplish all other mandated or necessary workloads, negatively impacting the public services supported by the revenue FTB generates.

As a result, FTB has begun a comprehensive review of resources, both positions and tools that support our technology work for all functions. This proposal focuses on resource gaps impacting privileged access and multi-factor authentication. As warranted, additional resource gaps may be addressed in other or future year Budget Change Proposals.

C. State Level Consideration

FTB's responsibilities include administering the income tax program on behalf of the state of California. FTB processes over 22 million returns and 10 million payments. Through these efforts, FTB collects approximately 77% of the General Fund, or approximately $190 billion annually.

Every technology that FTB implements must ensure the ongoing success of FTB's operations that support FTB's mission to help taxpayers file timely and accurate tax returns and pay the correct amount to fund services important to Californians.

FTB's Foundational Principles. Two of FTB's Foundational Principles are to "protect the privacy and security of data entrusted to us" and to "operate with transparency to maintain public trust and confidence." The security and access management tools requested through this BCP will be part of the operational foundation that enables FTB's mission and foundational principles.

FTB Strategic Plan Considerations. This proposal supports FTB's Strategic Plan goals:

Goal 1: Exceptional Service states, "Strive to continuously enhance our customers' experience." These new platforms and tools underpin critical services that FTB offers to both its enterprise and to taxpayers.

Goal 4: Operational Excellence states, "Optimize our processes, products, services, and resources to better serve our internal and external customers." Adopting modern security and access management tools mitigates emerging and evolving IT security threats, manages risks, and protects customer privacy and security.

SAM (State Administrative Manual) and SIMM (Statewide Information Management Manual) Compliance. PAM and MFA proposed improvements align with SAM and SIMM requirements.

D. Justification

It is imperative that FTB continues to strengthen its IT security posture in line with state-level direction to defend against increasing threats to FTB's sensitive and confidential data. As FTB continues to expand its portfolio of critical service offerings and access to confidential data to California taxpayers, FTB must remain vigilant to ensure the necessary security measures and operational insights are in place to prevent security breaches or significant disruptions to critical state services, damaging FTB's and the state's reputation and putting the state at risk for significant financial loss.

To fulfill the responsibility of complying with evolving security policies and standards and reducing departmental security risks, it is necessary for FTB to both modernize privileged access processes by implementing a PAM solution and improve login security for FTB's public website by implementing MFA.

Privileged Access Management (PAM):

FTB requests $794,000 in FY 2023-24, $553,000 in FY 2024-25, and $584,000 in FY 2025-26 and ongoing for OE&E funding, which includes software costs and consulting services in FY 2023-24 and software costs in FY 2024-25 and ongoing.

Access management is a vital part of ensuring the confidentiality, integrity, and availability of systems, applications, and data is maintained. This is especially true for privileged access, which permits the access required for critical work, such as monitoring planned IT system changes, and troubleshooting on FTB's confidential and sensitive systems.

In addition, the Cal-Secure Security Strategic Plan[2] roadmap specifically requires PAM and defines it as, "Secure provisioning of privileged access to critical assets, and effective monitoring and maintenance of privileged accounts and access."

Cal-Secure lists implementation of PAM as a high priority item. Because privileged user accounts have elevated permissions, the ability to change settings, and access to confidential data, they pose a significant target for cyber criminals, and therefore, risk to FTB. If compromised, severe damage could be caused not only to FTB's operations, but to FTB's reputation, due to data loss.

FTB currently has limited manual and automated processes to administer privileged access but not a PAM solution or all needed functionality. In a recent California Military Assessment, FTB received several findings and recommendations to improve the process. An enterprise-grade PAM solution would allow FTB to effectively monitor the entire network and provides insight into which users have access to what data. It is the best way to protect FTB's internal accounts from an attack by malicious parties who would then gain access to FTB's confidential and sensitive data.

FTB currently has a core, foundational implementation of CyberArk password storage functionality. FTB has evaluated PAM options and is requesting to expand our CyberArk investment to leverage their PAM capabilities. This Commercial Off the Shelf (COTS) enterprise solution will enable FTB to meet FTB's strategic objectives. CyberArk will be expanded to provide the following PAM capabilities:

- Secure user provisioning: The process of allocating privileges and permissions to users
- Credential protection: Privileged users will not know their password until they need it. The password is then provided to them by the PAM solution, with an expiration timeframe. Privileged users perform their work leveraging the password. When work is complete, the password is automatically changed by the PAM solution.
- Session isolation: A privileged user logs into a secure portal that initiates an isolated session, granting secure access to the protected resource.
- Session recording and auditing: The ability to record, store, and audit the activity that occurs during secure portal sessions provided by session isolation.
- Endpoint credential management: For local administrative accounts on servers and workstations, the ability to change passwords automatically and keep them secret until needed.

This protects a wide range of systems and infrastructure components from unauthorized access and tampering. It will also improve FTB's compliance with the following IT security policies and standards:

- California's Cal-Secure strategic initiatives
- Center for Internet Security (CIS) top 18 Critical Security Controls
- IRS Publication 1075
- NIST 800-53
- SAM 5300 security standards

This PAM solution ensures precise, just-in-time management of access controls, without interfering with FTB's 24x7 operability.

[2] https://cdt.ca.gov/wp-content/uploads/2021/10/Cybersecurity_Strategy_Plan_FINAL.pdf, page 18

Infrastructure Server Systems Unit
(Information Technology Specialist I – 2.0 permanent positions)

FTB requests two positions to implement and support the CyberArk solution for PAM. With the help of consulting services, the team will implement the new solution, receive real-time training, transition existing functions to the new solution, and maintain and continue to provide new services.

These positions will augment the Infrastructure Server Systems Unit existing positions and perform new work to configure and manage platforms, mature PAM, manage privilege session management, and conduct account discovery and provisioning. The staff will ensure availability and resiliency of the solution, that proper controls are in place, and that they do not unnecessarily interfere with mission-critical 24x7 services.

Specifically, the roles encompassed within these positions include:

CyberArk subject matter expert (SME): Helps design and architect all aspects and phases of the solution rollout. Assists with new platform onboarding (e.g., integration with other IT products), safe design, and onboarding additional CyberArk capabilities.

Vault Administrator: Works closely with the SME to understand and carry out new initiatives or onboarding of new CyberArk capabilities. Maintains the CyberArk Identity Security Suite, including, ensuring full operability of the application, creating policies, and executing project tasks defined by the SME.

Infrastructure Support: Manages the operating system (OS) and hardware that supports the CyberArk software. Ensures the hardware and OS is working within specifications, monitors services, performs backups, helps troubleshoot infrastructure issues, and conducts upgrades, migrations, and patching.

Data Administrator: Administers the CyberArk solution, including fulfilling requests for new safe creation, account and password uploads, and application definition.

Without these additional positions, FTB will not be able to perform this work.

Multi-Factor Authentication (MFA):

FTB requests $700,000 in FY 2023-24 and ongoing for OE&E funding, which includes software costs.

Authentication of users in any IT environment, including FTB's, is a vital part of ensuring users are validated before they are granted the appropriate access to data and information. FTB has initial identity proofing during account setup for FTB's public website applications. However, once an account is set up, authentication currently consists of only a single factor of a user ID and password combination. Lack of an additional factor for authentication leaves FTB non-compliant with FTB policy, IRS Publication 1075, SAM, and CDT's Cal-Secure policies, which leaves FTB vulnerable to attempts of account impersonation or possible fraudulent activity.

FTB proposes to integrate a cloud-based MFA method (adding another factor) by generating a passcode sent to the registrant and requiring the registrant to enter it into FTB's website application. Subsequently, the user may request to be remembered.

Enhancing these application logins with MFA will greatly strengthen security and thereby reduce the possibility of fraud and data loss. It will also bring FTB into compliance with the following IT security policies and standards:

- FTB Information Security Policy 9500, Section 215
- California's Cal-Secure strategic initiatives
- SAM Policy 5360, Identity and Access Management Section
- IRS Publication 1075

The MFA solution enhances FTB's IT security program as well as enables future integrations with registration and authentication processes of additional external customers. No additional staff resources are needed to implement and maintain MFA.

E. Outcomes and Accountability

The management of this effort will be the responsibility of FTB's Chief Information Officer (CIO) or a delegate. The fiscal oversight of the resources will be the responsibility of both the CIO and the Chief Financial Officer.

The CyberArk and MFA implementation is an expansion of solutions that meet FTB's operational needs. Fully implementing these new tools provides increased compliance with statewide security policies and industry standards and supports FTB's strategic goals.

FTB will procure its license renewals with a fully funded budget and manage the software timely to the needs of the department and in compliance with all policies.

F. Analysis of All Feasible Alternatives

Alternative 1: Approve FTB's request for $1.8 million, $1.77 million General Fund and $35 thousand special funds for two permanent positions and software costs in FY 2023-24; $1.6 million, $1.57 million General Fund and $30 thousand special funds for two permanent positions and software costs in 2024-25 and ongoing to reduce security risk by implementing a solution to automate PAM functions and improve login security by integrating MFA into FTB's public web applications in compliance with Cal-Secure direction.

Pros:

- Aligns with FTB, state (Cal-Secure), and federal IT security policies for PAM and MFA.
- Implements PAM to reduce risk associated with privileged accounts
- Integrates MFA, a recognized standard, into FTB's public web applications will meet taxpayer expectations for strong security in government systems with personal data.

Cons:

- Ongoing FTB expenditure and allocation from the state.

Alternative 2: Approve FTB's request for $1.8 million, $1.77 million General Fund, $30 thousand special funds for two limited-term positions and software costs in FY 2023-24; $1.6 million, $1.57 million General Fund, $30 thousand special funds for two limited-term positions and software costs in 2024-25 and 2025-26; and $1.3 million, $1.27 million General Fund, $30 thousand special funds for software costs ongoing to reduce security risk by implementing a solution to automate PAM functions and improve login security by integrating MFA into FTB's public web applications in compliance with Cal-Secure direction.

Pros:

- Aligns with FTB, state (Cal-Secure), and federal IT security policy for PAM and MFA.
- Implements PAM to reduce risk associated with privileged accounts
- Integrates MFA, a recognized standard, into FTB's public web applications will meet taxpayer expectations for strong security in government systems with personal data.

Cons:

- Ongoing FTB expenditure and allocation from the state.
- Premature loss of knowledge, capacity, and momentum as staff in limited-term positions find fulltime work and leave the limited-term position prior to the expiration of their limited term.
- Loss of knowledge as limited-term positions expire.
- Inability to maintain, monitor, and provide ongoing support of CyberArk capabilities after limited-term positions expire.

Alternative 3: Do not approve the request.

Pros:

- No increase of FTB's expenditure or allocation from the state.

Cons:

- FTB will not be able to leverage modern security and access management tools to mitigate emerging and evolving IT security threats, manage risks, and protect customer privacy and security.
- Increased risk of unauthorized access to taxpayer information and potential threat of fraudulent activity.
- FTB will not be able to improve its security stance in compliance with Cal-Secure and other policies.

G. Implementation Plan

2023-24:

- July 1, 2023 – Funding provided.
- Hire new positions and onboard for CyberArk workloads.
- Install and configure initial CyberArk privileged user account capabilities.
- Implement MFA.

2024-25:

- July 1, 2024 – Funding provided.
- Install and configure additional CyberArk service account capabilities.
- Expand usage and coverage of CyberArk

2025-26:

- July 1, 2025 – Funding provided.
- Install and configure additional CyberArk application account capabilities.
- Expand usage and coverage of CyberArk

H. Supplemental Information

None

I. Recommendation

Approve FTB's request for $1.8 million, $1.77 million General Fund and $35 thousand special funds, for two permanent positions and software costs in FY 2023-24: $1.6 million, $1.57 million General Fund and $30 thousand special funds, for two permanent positions and software costs in 2024-25 and ongoing.

This funding and staffing will enable FTB to purchase an enterprise-grade PAM solution that will allow new resources, with the help of consulting services, to augment and mature PAM in compliance with Cal-Secure and other policies. And the funding will enable the purchase and implementation of MFA for FTB's public web applications.

BCP Fiscal Detail Sheet

BCP Title:

BR Name:

Budget Request Summary

Personal Services