STATE OF CALIFORNIA
Budget Change Proposal - Cover Sheet
DF-46 (REV 06/19)

Fiscal Year	Business Unit	Department	Priority No.
2021/22	7730	Franchise Tax Board	2

Budget Request Name	Program	Subprogram
7730-002-BCP-2021-GB	6280/6290/6295	6280010/6280019

Budget Request Description
Privacy and System Assessments

Budget Request Summary

The Franchise Tax Board (FTB) requests 12 permanent positions and $1.6 million General Fund and $69,000 Special Funds in 2021-22; and $1.5 million General Fund and $64,000 Special Funds in 2022-23 and ongoing. These resources will accommodate newly mandated state and federal workloads within the critical functions of FTB's Privacy Program and Information Security Oversight Unit (ISOU). The requested positions will support enhanced levels of effort required under Federal Publication 1075 and conduct the newly mandated Privacy Threshold Assessments (PTAs), Privacy Impact Assessments (PIAs) and System Security Plans (SSPs) to ensure that FTB meets the state and federal mandates. The resources will play a key strategic role in ensuring that FTB expands and validates the privacy, security framework, reportable technology projects, and security measures for the department's business processes, projects and systems.

Requires Legislation	Code Section(s) to be Added/Amended/Repealed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

Pending Board Approval

Department Director	Date	Agency Secretary	Date

Department of Finance Use Only

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

PPBA	Date submitted to the Legislature

A. Budget Request Summary

The Franchise Tax Board (FTB) requests 12 permanent positions and $1.6 million General Fund and $69,000 Special Funds in 2021-22; and $1.5 million General Fund and $64,000 Special Funds in 2022-23 and ongoing. These resources will accommodate newly mandated state and federal workloads within the critical functions of FTB's Privacy Program and Information Security Oversight Unit (ISOU). The requested positions will support enhanced levels of effort required under Federal Publication 1075 and conduct the newly mandated Privacy Threshold Assessments (PTAs), Privacy Impact Assessments (PIAs) and System Security Plans (SSPs) to ensure that FTB meets the state and federal mandates. The resources will play a key strategic role in ensuring that FTB expands and validates the privacy, security framework, reportable technology projects, and security measures for the department's business processes, projects and systems.

B. Background/History

Currently, under the direction of the Chief Security Officer (CSO), the implementation of FTB's Privacy and Information Security Programs are executed by the Privacy, Security, and Disclosure Bureau (PSDB). PSDB develops policies and procedures to ensure the safety and security of FTB's employees; the confidentiality, integrity and availability of FTB's information systems and the information contained within and the privacy of the personal data collected and used by department. FTB's Chief Privacy Officer (CPO) is responsible for numerous functions regarding the department's responsibility to protect confidential and sensitive data and to ensure the enterprise is collecting, using and sharing data appropriately. The CPO promotes awareness of and ensures the privacy of employee and taxpayer data, and appropriate use of FTB data that meets federal and state requirements mandates, laws and regulations.

In the last 12 months, 3 significant new federal and state mandates related to enhanced security and privacy reviews and controls were issued in draft form or were adopted. These requirements are, or soon will be, required to be performed as described in the various procedures. They are as follows:

- **Draft Publication 1075 – issued with an effective date of December 1, 2019 and expected to be finalized in September or October of 2020.**

  Internal Revenue Service (IRS) requirements stated in the draft Publication 1075, effective December 2019, requires FTB to review and provide analysis for privacy requirements to develop and disseminate an enterprise–wide privacy program plan. This plan should include a description of the privacy program, management's commitment to compliance, strategic goals and objectives and identification and implementation strategies for ongoing efforts to meet these objectives. The plan must include policies and procedures that address the use of Personally Identifiable Information (PII) for internal testing, training and research (updated IRS Publication 1075).

  Failure to adhere to these standards risks FTB's ability to obtain critical return information from the IRS that is used to process over 19 million California tax returns and supports the generation of over $4 billion in compliance revenue annually.

- **State Administrative Manuel (SAM) 5310.8/SIMM 5310-C mandates, effective August 2019 and revised November of 2019.**

  Under the provisions of SAM 5310.8 and SIMM 5310-C, FTB's Privacy Program is now required to conduct PIAs on business processes, projects and systems that involve the

collection, creation, maintenance, distribution or disposal of personal information as defined in Civil Code section 1798.3. The objective of a PIA is to identify privacy risks and protections throughout the life cycle of personal information collected to support business processes. PIAs are also conducted to ensure that programs or information systems that contain or use personal information comply with legal, regulatory, and policy requirements regarding privacy. As required by the new mandates, in order to protect personal information, information asset owners are required to apply all applicable statewide and state entity information privacy and security mandates, laws, policies, standards, and procedures. This includes conducting a PTA and, if necessary, a PIA when the collection, use, maintenance, storage, sharing, disclosure or disposal of personal information (as defined by Civil Code section 1798.3) is involved. State entities are required to use the State Information Management Manual (SIMM) 5310-C, which defines PTAs and PIAs, or an equivalent tool to meet this requirement.

Failure to adhere to these mandates results in FTB being out of compliance with statewide mandates and subjects FTB to both audit findings and the inability to timely identify privacy gaps and risks which ultimately could result in a data breach or the erroneous retention and use of personally identifiable information.

- **State Administrative Manuel (SAM) 5305.5/SIMM 5305-A Mandates, effective January 2018.**

  FTB's current security program requirements include planning, oversight, and coordination of information security program activities to effectively manage risk, provide for the protection of information assets, and prevent illegal activity, fraud, waste, and abuse in the use of information assets. This workload is managed by the department's Information Security Program. FTB's assessment process has two goals: 1) determine the privacy risks and effects of collecting, maintaining, using, and disclosing personal information; and 2) evaluate protections and alternative processes for handling personal information to eliminate or mitigate potential privacy risks. In general, FTB's current program focuses on common grouping of programs and system security plans have been developed for these broad groups. Under SAM 5305.5, FTB is required to complete and file System Security Plans for all critical state systems versus common groupings.

  Failure to adhere to these mandates results in FTB being out of compliance with statewide mandates and subjects FTB to audit findings and the inability to identify privacy gaps and risks as required which ultimately could result in a data breach to our systems.

Each of these mandates have common requirements but also distinct requirements. Each needs to be done and the completion of one of these mandates does not eliminate the need to do the other mandated reviews. FTB resources work together to ensure the reviews work in tandem but also allow for consideration of unique factors and the completion of all mandated documents.

Following are the Workload History charts for the two program areas involved with ensuring FTB's personally identifiable information is secure within business processes, projects and systems.

Privacy, Disclosure and Safeguard Section Workload History

Workload Measure	2015-16	2016-17	2017-18	2018-19	2019-20
Business PTAs/PIAs	N/A	N/A	N/A	N/A	51
System PTAs/PIAs	N/A	N/A	N/A	N/A	0
Project PTAs/PIAs	N/A	N/A	N/A	N/A	3

Security Operations Workload History

Workload Measure	2015-16	2016-17	2017-18	2018-19	2019-20
New System Security Plans (SSPs) Completed	N/A	N/A	N/A	N/A	6
System Security Plans Updates	N/A	N/A	N/A	N/A	0

C. State Level Considerations

This request is aligned with the CDT's Strategic Plan Vision 2020: Improve and invest in security capabilities to protect mission-critical systems and data. The strategic plan identifies five top priorities. Two of those priorities focus on privacy and information security.

This proposal also supports FTB's Strategic Plan Goal #4, Operational Excellence, strategy of "mitigating emerging and evolving threats and managing risks to maintain taxpayer privacy and security." This request also aligns with FTB's foundational principle to "protect taxpayer information and privacy" which supports the department's mission and guides the work needed to achieve goals and implement the strategies as outlined in the department's Strategic Plan.

Safeguarding privacy and data security is, and should remain, a top priority in data exchange, storage, and use efforts. FTB must continue to heighten the focus on oversight and enforcement of privacy and security protections to ensure that the department's systems and contractors effectively safeguards individuals' confidential and other sensitive personal information. This must entail continued compliance reviews to ensure adoption of adequate privacy and security standards.

D. Justification

This proposal requests resources necessary for FTB to comply with privacy mandates and standards from the CDT OIS and the IRS. Conforming to these new requirements and the evolving changes to privacy and security landscapes increases workloads and requires establishing appropriate controls that protect the privacy and security of each FTB asset. Under the new CDT mandate and IRS requirements, FTB must engage in the new or expanded program efforts. FTB possesses approximately 776 IT systems with PII data incorporated within that are subject to both PTA/PIA and SSP documetation.

- Enhance and disseminate an enterprise-wide privacy and sercurity program responsible for reviewing and providing analysis for all privacy and security requirement interpretations. IRS Publication 1075
- Develop and implement specific policies and procedures to address the use of PII in internal testing, training, and research. IRS Publication 1075
- Develop and implement specific policies and procedures that adhers to security controls identified in the SSP per state and federal information security laws under all of the following authorities.
    1. IRS Publication 1075
    2. SAM Information Asset Management - 5305.5
    3. Federal Information Processing Standard Publication 199
    4. California Department of Technology's Audit Finding

5. National Institute of Standards and Technology: SP 800-53
6. California SIMM 5300-A

- Establish, maintain and annually re-certify enterprise information systems per controls identified in an SSP.
- Establish, maintain, and annually update an inventory of all programs and systems that create, collect, use, process, store, maintain, disseminate, disclose or dispose of PII. IRS Publication 1075: Program Management
- Complete an initial and annual PTA/PIA on all FTB businesses processes, systems and reportable IT projects. SAM 5310.8/SIMM 5310-C
- Expanded level of work to oversee, coordinate and facilitate audits by external entities, such as the IRS, military, or CDT.
- Expanded level of education and outreach activities to internal business partners.
- Expanded level of collaboration with external agencies on privacy and security related topics, trends, and issues.

If the department does not comply with the new IRS mandates, the privilege to use Federal Tax Information (FTI) provided by IRS could be revoked. This revocation could result in an annual revenue loss.

In addition to complying with the mandates, this request will strengthen FTB's ability to expand and maintain a compliance program that effectively mitigates internal and external security threats and stays up-to-date with the latest regulatory changes. It enables the department to evaluate and measure current privacy and information security measures.

To strengthen FTB's strong privacy practices and assist with protecting personal information, the department requests resources for the department's Privacy Program and Information Security Oversight Unit.

Privacy Program
1 Administrator II, 1 Sr. Operations Specialist, and 5 Staff Operations Specialist

The PSDB develops policies and procedures to ensure the safety, security, confidentiality, integrity and availability of FTB's information systems. The privacy and protection of the personal data collected and used by the department is managed by providing the following:

- Expanded review of business processes to ensure all PII collected is authorized, documented, used, protected, and disposed of appropriately.
- Coordination and completion of PTAs and PIAs – involves analyzing PTA and PIA questionnaires, drafting final reports, and following up on compliance. SAM 5310.8/SIMM 5310-C
- Plan, oversee and direct staff workloads – requires maintaining good communication with impacted internal and external stakeholders to ensure the exchange of information critical to operational goals.
- Expanded education and outreach activities.
- Expanded collaboration with external agencies on privacy related topics, trends, and issues.

The required PTAs and PIAs assist information owners, program managers, and system owners with incorporating privacy protections into the development and management of state information assets and records. Staff collaborate with the subject matter experts to first complete a PTA which consists of 16 questions. If the threshold in the PTA is met, a PIA follows with another 55 questions. The requested staff will be responsible for ensuring the department meets the new requirements to expand the privacy program and conduct required PTAs and PIAs on an annual basis on business processes, projects and systems.

The new federal mandates and the increase of the privacy requirements, outlined in the IRS Publication 1075, require FTB to address these mandated requirements, while still allowing the department to address the ever-changing demands of protecting FTB's confidential, sensitive and PII. The Privacy Program must ensure the appropriate privacy controls are incorporated into the department's projects, business processes, and systems. To meet these escalating demands, FTB needs additional Privacy Program staff to manage the privacy workloads. Having the dedicated resources to complete these workloads will ensure FTB's compliance with applicable state and federal laws, mandates, Technology Letters, regulations, policies, standards, guidance, and organization-specific issuances. Adherence requires the Privacy Program to:

- Follow the IRS' requirement, as mandated by the new Publication 1075, of developing a Privacy Program Plan and establishing, maintaining and updating an inventory of all programs and systems that create, collect, use, process, store, maintain, disseminate, disclose or dispose of PII.
- Ensure the purpose of collecting PII is clearly communicated at, or prior to the time of collection, and any subsequent use is consistent with the original purpose while ensuring relevant personal information is collected by lawful means.
- Ensure PII is not disclosed without consent, unless authorized by law.

While adhering to state, federal and regulatory privacy mandates and requirements, FTB would be incorporating an additional layer to the department's information security measures.

Information Security Oversight Unit

1 IT Supervisor II, 1 IT Specialist II and 3 IT Specialist I

The ISOU team members are the department's information security subject matter experts and provide the following:

- Support and oversight to departmental projects, task forces, and initiatives.
- Consult with departmental program areas and project teams to ensure compliance with Information Security Policies and industry best practices for system and network design issues.
- Identify and recommend risk mitigation strategies.
- Maintain the Information Security Policy and Standards.
- Information Security awareness training for the department.
- Cybersecurity review of contracts, inter-agSency agreements, and pending legislation.
- Information Security Assessments and Audit finding facilitate and remediate.
- Evaluate existing and new systems for improvement of information security.
- Document security strategies, requirements, and controls in SSPs.

As identified in SAM 5305.5/SIMM 5305-A, SSPs are a tool used to perform risk assessments for a system. The risk assessment identifies potential threats and vulnerabilities in an information system, determines expected risks and analyzes planned or actual security controls and potential impacts on operations and assets. To facilitate compliance and implementation of the controls suite, a prioritized baseline of information security controls was developed using the catalog in the NIST Special Publication 800-53, Rev. 4. The IRS 1075 publication, SAM 5300, FTB's Risk Management Framework (RMF), and security best practices were used to determine the required controls for FTB's environment.

FTB possesses approximately 776 IT systems. To date, the department has a completed SSP for six categorized and classified major areas of work systems versus an SSP on all 776 systems. Based on the mandates noted in SAM 5303.5/SIMM 5305-A, an SSP is required on every system. In a review by CDT, they also confirmed the requirement . An SSP is a document that describes security requirements and the security controls of the system for meeting those requirements. To address the CDT OIS's finding, be fully compliant with this requirement, and review each system in detail for unidentified security gaps, FTB will need to complete an SSP for each of its approximately 776 IT systems. In addition, CDT OIS observed that once these SSPs are initially completed an annual recertification for each IT system is also required, per SIMM 5300-C.

Each SSP is completed by documenting 197 different security control requirements, describing how the system meets those requirements, and providing evidence that the requirement is met. The complexity of controls and FTB's systems results in significant consultations with the technical areas and review of the plan for the SSP to be completed thoroughly and appropriately. Completing an SSP for the first time requires:

- Significant consultations and reviews with the technical owners of the system.
- Explanation of the SSP and security controls to them - the security expert must learn the unique aspects of the system and assess their adherence to security controls.
- Updating each SSP whenever a system changes or at least annually.

In order to complete this new and ongoing permanent work, the ISOU needs the requested seven additional resources. The 3 IT Specialist I staff members will complete the majority of the SSPs. The IT Specialist II will be the primary process and tool administor, handle the most complex SSPs and assists with escalated SSPs from an IT Specialist I. Adding these positions to the Information Security Oversight Unit will put the direct reports of the unit manager at 17. Considering the enterprise scope, significant complexity, and impact of this workload, the ISOU manager should not have that many direct reports. As such, an IT Supervisor II is needed to manage the Application Security and Security Audit Logging functions of the unit.

E. Outcomes and Accountability

This proposal will ensure staffing levels correspond with the degree of oversight, attention to detail and timeliness required to meet the demands of the complex and sensitive PII workloads. It will also ensure compliance with federal and state policies, mandates, laws and regulations. Approval will allow FTB to ensure mission critical staffing needs are met and maintained.

The management of resources received from this proposal will be the responsibility of the Chief of the Administrative Services Division or a delegate. The fiscal oversight of the resources is the responsibility of the Chief Financial Officer.

Privacy, Disclosure and Safeguard Section Projected Outcomes

Workload Measure	2019-20	2020-21	2021-22	2022-23	2023-24	2024-25
Business PTAs/PIAs	51	83	83	83	83	83
System PTAs/PIAs	0	0	260	490	670	776
Project PTAs/PIAs	3	3	3	3	3	3

Security Operations Projected Outcomes

Workload Measure	2019-20	2020-21	2021-22	2022-23	2023-24	2024-25
New System Security Plans (SSPs) Completed	6	0	260	230	180	106
System Security Plans Updates	0	0	0	260	490	670

F. Analysis of All Feasible Alternatives

Alternative #1: Approve 12 permanent positions, $1.6 million General Fund and $69,000 Special Funds in 2021-22 and $1.5 million General Fund and $64,000 Special Funds in 2022-23 and ongoing.

These resources will allow FTB to meet the increased demands for ensuring that the appropriate levels of privacy and information security controls are in place to protect the privacy and confidentiality of data. By expanding a privacy compliance program and implementing a Privacy Program, as mandated, the department will be able to continue with a preventative approach to protecting the information from data breaches. In turn, the department will meet the increased state and federal privacy policies, mandates, laws, and regulations.

Alternative #2: Approve $1.4 million General Fund and $58,000 Special Funds in 2021-22 and $1.3 million General Fund and $54,000 Special Funds in 2022-23 and ongoing to support 10 permanent positions:

These resources will allow FTB to meet some of the increased mandate requirements for ensuring that the appropriate levels of privacy and information security controls are in place to protect the privacy and confidentiality of data. This alternative would lead to a reduction in the amount of required work the department could accomplish and will not allow FTB to gain compliance with state mandates or IRS requirements.

Alternative #3: Approve 6 permanent positions, $822,000 General Fund and $35,000 Special Funds in 2021-22 and $756,000 General Fund and $32,000 Special Funds in 2022-23 and ongoing.

This alternative reduces the number of permanent positions needed. This alternative will not provide the resources needed to fully comply with privacy and information security policies, standards, mandates, laws and regulations in a timely manner.

Alternative #4: Do not approve the request for additional resources.

Should the BCP be denied, it will impact the Privacy Program and Information Security Oversight Unit's ability to expand information security workloads and meet the new mandates and requirements set forth by CDT OIS and the IRS. FTB will not be able meet the requirements to complete PTAs, PIAs and SSPs to identify privacy problems and take effective counter-measures before problems become a privacy crisis. The department's inability to conduct these assessments and determine privacy risks and place controls that protect the PII being collected, used, maintained, shared, stored and disposed of puts the department at risk.

Moreover, denial of this proposal compromises FTB's confidentiality requirements, integrity, and availability of the information systems and risks improper disclosure of data. As such, FTB and the state would be open to various liabilities and/or embarrassment.

G. Implementation Plan

June 2021 - All documents to establish permanent position are prepared and approved by the FTB Budget Officer and forwarded to Department of Finance.

June 2021 - Department of Finance notifies FTB of position approval.

July 2021 - Permanent positions are established and FTB begins hiring.

H. Supplemental Information

I. Recommendation

Alternative #1 is recommended: Approve 12 permanent positions, $1.6 million General Fund and $69,000 Special Funds in 2021-22 and $1.5 million General Fund and $64,000 Special Funds in 2022-23 and ongoing.

This proposal will allow FTB to meet the increased demands for ensuring that the appropriate levels of privacy and information security controls are in place to protect the privacy and confidentiality of data. By expanding a privacy compliance program and implementing a Privacy Program, as mandated, the department will be able to continue with a preventative approach to protecting the information from data breaches. In turn, the department will meet the increased state and federal privacy policies, mandates, laws, and regulations.