| Fiscal Year | Business Unit | Department | Priority No. |
|---|---|---|---|
| 2021-22 | 7502 | California Department of Technology | 1 |

| Budget Request Name | Program | Subprogram |
|---|---|---|
| 7502-017-BCP-2021-A1 | 6230 | N/A |

**Budget Request Description**
Digital Identification

**Budget Request Summary**

The California Department of Technology (CDT) requests 2.0 positions and $1,111,000 in General Fund (GF) in Fiscal Year (FY) 2021-22 and FY 2022-23 to deploy a Digital Identification (ID) ecosystem for an initial subset of state services that will provide a consistent, secure, privacy enabled, reliable, and consent-based method to authenticate and verify the identity of a California resident when accessing the subset of digital state services. Using an iterative approach, this initial Digital ID ecosystem and deployment will provide invaluable information needed to develop a roadmap for Digital ID expansion across all state services.

| Requires Legislation | Code Section(s) to be Added/Amended/Repealed |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

| Does this BCP contain information technology (IT) components? ☐ Yes ☐ No<br>*If yes, departmental Chief Information Officer must sign.* | Department CIO<br>N/A | Date<br>N/A |
|---|---|---|

**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.** N/A **Project Approval Document:** N/A

**Approval Date:** N/A

**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 |
|---|---|---|---|
| Kimberly Crabtree<br>Kimberly Crabtree (Apr 1, 2021 21:43 PDT) | 3/23/2021 | Manveer Bola<br>Rick Klau (Apr 1, 2021 21:57 PDT) | 3/23/2021 |
| **Department Director** | **Date** | **Agency Secretary** | **Date** |
| Amy Tong<br>Miles Burnett (Apr 2, 2021 07:50 PDT) | 3/23/2021 | Yolanda Richardson<br>Justyn Howard (Apr 2, 2021 09:27 PDT) | 3/23/2021 |

**Department of Finance Use Only**

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

| PPBA | Date submitted to the Legislature |
|---|---|
| Evelyn Suess | 4/1/2021 |

## A. Budget Request Summary

The California Department of Technology (CDT) requests 2.0 positions and $1,111,000 in General Fund (GF) in Fiscal Year (FY) 2021-22 and FY 2022-23 to deploy a Digital Identification (ID) ecosystem for an initial subset of state services that will provide a consistent, secure, privacy enabled, reliable, and consent-based method to authenticate and verify the identity of a California resident when accessing the subset of digital state services. Using an iterative approach, this initial Digital ID ecosystem and deployment will provide invaluable information needed to develop a roadmap for Digital ID expansion across all state services.

In alignment with the Governor's Budget and Vision 2023 goals, the user experience needs to be simplified for California residents by allowing access to state services through a single digital identifier; therefore, eliminating the need to repeatedly prove their identity and manage multiple user IDs to obtain services. Considering there are hundreds of state services, we need to first establish the foundational Digital ID ecosystem and then deploy to a subset of state services. This initial effort will prove the ecosystem works effectively and is scalable, as well as identify the best path to integrate the Digital ID ecosystem with the many technologies that deliver existing state services today.

## B. Background/History

The State of California has published its strategic technology plan entitled Vision 2023 which outlines the current challenges facing the more than 200,000 state employees whose mission is to provide a wide array of services to the nearly 40 Million California residents.

The recent health crisis starkly underlined the importance of being able to quickly deliver on emergency relief efforts for its residents and to adapt the IT infrastructure to support spontaneous and at times exponential growth in services demand while maintaining a high level of data security, privacy and availability. With over 150 departments and more than 300 often complex English-language only websites, navigation for less affluent residents or for non-native English speakers representing close to 16 million Californians can be overwhelming.

The state desires to consolidate its technology, making it simpler, more accessible and more consistent in data protection and security. Greater collaboration and easier contact management has also been identified. The state also desires to embrace modernization that can adapt to and leverage market advances in bandwidth, familiarity and accessibility.

When addressing security and regulatory requirements, the state's Vision 2023 outlines a number of challenges it wishes to address such as meeting the requirements for privacy and the Information Practices Act, a desire to simplify resident on-boarding and services enrollment, with strong anti-fraud protection and the ability to support innovative and simple to use strong authentication.

Online residents have an expectation of speed of service with convenience. Online services require consistent and accurate identification in order to protect privacy and deliver a seamless experience. Today every state program delivers services independently with an inconsistent digital experience resulting to the detriment of some of our most vulnerable Californians depending on a seamless interaction to attain a service. Where services rely on proving who you are, breakdowns in disjointed technology operations between state entities have led to unacceptably slow or unusable service. This is commonly due to inconsistent implementation of identity verification and authentication services which would otherwise support a seamless digital user experience.

Multiple unconnected systems for users to authenticate their identity mean that users must repeatedly prove their identity across programs. This does not meet users' expectations who see government as a single entity.

Departments rely on a myriad of sources to authenticate the identity of a California resident accessing services. For example, health care programs track eligibility differently. Some use a Client Index Number (CIN), others use an SSN or MEDS-issued pseudo, and others rely on County consortium systems. Systems also lack the capability to update resident information when they move. Resident information is parsed out to various applications within the system. This data may become inconsistent over time, as a member changes his or her address or has life or employment events.

Inconsistency in the source and process of authenticating a resident's identity, coupled with a lack of agreement on what constitutes the unique record identifier creates redundancies, increases errors and security gaps, introduces opportunities for fraud and abuse, compounds costs, and causes delays and frustrations to residents.

Programs and departments are independently responsible for implementing, maintaining, supporting and securing multiple identity verification and authentication systems, when identity verification and authentication is a common need.

The background for each area requesting resources is detailed below, in order to augment current Office of Technology Services (OTech) resources that have digital ID expertise, related to current state services/solutions:

The Office of Enterprise Technology (OET) manages and delivers IT State services and information to enhance digital government that works for all Californians by providing foundational platforms and technology (such as Geographical Information System (GIS)/Open Data, Web Portals, Software Engineering and Open Source code curation). Expertise among OET staff is varied including front-end and server side developers, UI/UX skills, GIS specialists, data engineering/analytics and DevOps engineering. OET also hosts various communities of practice to foster emerging technologies and help CDT's partners understand issues impacting the state.

## C. State Level Consideration

This request aligns with goals outlined as part of the California Technology Strategic Plan, Vision 2023:

**Make common technology easy to access, use, share and reuse across government (Goal 3)**

Vision 2023 states that to deliver value to users more quickly, we must pool our investments and efforts into a shared digital infrastructure. We can do this by using common technology that can be adapted, shared and reused across the state. For most common problems, this will mean developing a suite of demonstrated approaches to be used by default, unless exceptions are met.

Centralizing and standardizing on common technology choices makes it easier for the State to take advantage of its scale as the world's fifth-largest economy. By leveraging the state's size, we can deliver better services at a responsible cost and use public funds to better serve Californians. This does not mean locking the state into a single choice, or vendor, or inflexible static standards. It means understanding user needs and providing managed choices and flexibility. Most importantly, achieving this goal will make it faster and easier for teams to solve

actual problems for our residents, such as receiving emergency grant funding, starting businesses or finding childcare.

Goal 3 includes the Challenge 3.5: How can we develop a more secure, reliable and consistent way for people seeking state services to prove who they are?

Delivering options for a common approach to identity verification and authentication is the right first step and requires significant work to understand the public's needs and expectations for privacy and security, how and when government shares information, transparency about information and information sharing, and informed consent. This project provides Californians the ability to opt-in and maintain control of their identify information as they enroll to receive state services. Similarly, significant work is required to understand program, departmental, agency and statewide needs.

This request also aligns with the Governor's Proposed 2021-22 Budget:

**Digital Transformation and Results-Oriented Government**

One of the significant projects mentioned under Modernize and Improve the User Experience section in the Governor's Budget is researching the development of a Digital ID system to be used across all state departments. This project is one of the many next steps identified to modernize and improve the way in which individuals engage with state government.

Building upon the state's 2019 investment in digital innovation, the Governor called upon CDT to accelerate the digital transformation of services and how they are delivered to nearly 40 million Californians by working collaboratively with state agencies and departments to find innovative ways to adapt and deliver core government functions online while improving business processes and consumer interactions.

The events of 2020 highlighted the urgent need to modernize government services in an online environment. The state recognizes the need to optimize technology infrastructure and investments, foster digital services, and use data to inform decision-making. Government modernization will lead to improved and equitable decisions, services, and outcomes for Californians.

**Privacy and Security Considerations**

The Digital ID ecosystem will be architected to deliver program efficiencies and a seamless user experience for residents accessing government services, while prioritizing user consent and privacy, and ensuring the highest levels of security for the data involved. The ecosystem will be fully compliant with state and federal statutes and policies applicable to the type of resident information collected for purposes of authentication, including but not limited to the Information Practices Act (IPA) and Health Insurance Portability and Accountability Act (HIPAA). Privacy controls include the following:

1. Resident will be required to consent to and designate each service that is authorized to receive personal information provided for the creation of the digital id.
2. Resident information required for authentication will be program specific and obtained incrementally on an as-needed basis.
3. Resident information will be provided to departments for designated purposes only.
4. Law enforcement will be required to obtain a subpoena, search warrant or other legal process to access the information in the system.
5. Information collected from residents will be customized to the program requirements for authentication.
6. Resident information uploaded for authentication purposes will be deleted after their identity has be confirmed.

7. Security controls will be implemented to match the Impact Level of the information collected. Data will be further protected through encryption and tokenization.

**D. Justification**

The residents of California must currently navigate across hundreds of websites managed by over 150 departments, with no cohesive registration or authentication. The experience for residents has been frustrating and rife with errors as they are forced to re-register, often with a completely different enrollment experience and credential requirements, including in-person registration for many services.

Providing digital services to the public relies on digital identification. This is a problem that every department independently solves differently, frustrating the public and introducing unnecessary cost, fraud, high risk security gaps, and complexity to the State's digital infrastructure. These issues have come to the forefront both throughout the COVID-19 pandemic, as demand for digital state services has rapidly increased, as well as the Department of Motor Vehicles and Employment Development Department modernization efforts where each has included identity proofing as a key component of the efforts. State agencies have eroded public confidence through the exposure of fraud. Remote services are no longer a luxury, but a necessity, not just due to our current pandemic, but because of the reality of California's extremely large geography and the need to serve remote populations. California residents typically have multiple login accounts, ways of registering, and validating their identity to receive the services they are entitled to receive.

Transforming state services to be digital by default necessitates investing in the common infrastructure required and making it easier for government employees to collaborate and work across silos. This will require CDT to lead the investment in a common infrastructure and building and enforcing simple, useful standards of excellence. To streamline services and create a simple, clear, consistent and secure user experience, CDT will be responsible for maintaining the Digital ID ecosystem across state services.

Many states, such as Colorado, have taken an iterative approach to address Digital ID within one agency or department, and extending the benefits of Digital ID across multiple agencies and departments upon completion.

CDT will begin developing one digital identifier across California's state government technology systems in a consistent, unified, and more secure approach resulting in the minimization of duplication in less mature identity management processes operated in a silo within each department today. This approach will provide a higher level of assurance to ensure the most appropriate, seamless, and equitable service experience is delivered while mitigating the opportunities of fraud and abuse by malicious actors. Developing a centralized functional Digital ID ecosystem for public-facing services is a foundation of the State's ability to provide digital services in a consistent manner. Deployment of the Digital ID ecosystem to a subset of state services will be the first step in the State's Digital ID journey that will expand to all state services.

CDT requests 2 positions, and $500,000 in consulting support to develop, execute and maintain a Digital ID ecosystem for a subset of state services.

Positions requested include:

- 1 Digital ID Product Owner (one CEA)
    - The CEA will develop and champion product vision, strategy, and roadmaps for multiple complex Digital ID ecosystem product lines, in support of business goals and objectives. They will also present and clearly articulate the Digital ID strategy and

roadmaps to State leadership. From the highest strategic view, the CEA will plan and execute effective new product opportunities and service enhancement(s).

- 1 business relationship manager (BRM) (one IT Specialist II)
    - The BRM will lead the partnership with state entities to build and evaluate business cases to support integration and migration/onboarding with the Digital ID product investment decisions. They will also collaborate with government service business programs, user experience and engineering teams to assess value, usability and feasibility of product features that meet business needs.

Given the importance of this statewide service, with its implications for the ways that Californians engage with government, an executive product owner at the CEA level is critical to ensure this effort has sufficient policy experience and ability to lead product development decisions across government departments and agencies. Also, since the Digital ID ecosystem provides value across the State, General Fund will be the best source of funding.

The recognized critical need for digital identification means that agencies and departments are independently investigating solutions. By taking on this effort for the State, CDT will not only reduce duplication of effort and further bifurcation of data but will allow agencies and departments to focus more on the services they provide.

CDT's initial proposed Digital ID ecosystem will mitigate the challenges state entities are facing with authentication and identity proofing and also create an extensible foundation for a single entity to provide the ecosystem to support services across the state. By transforming the way records are maintained, we streamline access and reduce risk from identity duplication.

This effort will ultimately lead to a single identifier for residents that is consent driven, privacy enabled, secure, reliable, and may be consistently used across all domains of state services. The effort will improve convenience for the residents, enhance user experience, increase efficiencies, eliminate duplicate payments, and reduce program fraud and associated costs.

As secure data storage is critical to the state, this initial Digital ID ecosystem will address security and privacy and compliance with all applicable regulations. The ecosystem is aimed towards making access to services easier for the average resident, without forcing a particular technology, in order to close the digital divide and increase inclusiveness and equity.

## E. Outcomes and Accountability

Key factors that will support improving user experience for Californians include service harmonization. Having a unique digital identifier and proven identity for residents will enable better integration across state programs; this will support resident experience on several levels. First, it provides opportunities to facilitate cross-program enrollment, and standardize point of entry to services. Second, it provides a data mechanism to allow consolidation of resident data across sources and maintained in a central location. The central maintenance of this information will also facilitate the creation of one or more public-facing portals to support real-time client access via a trusted verification service to both their current program and demographic information, as well as historical data.

CDT will build solid digital and technological foundations by focusing on critical shared services and statewide policy outcomes. This Digital ID effort will reduce the number of separate digital identification contracts and approaches and improve the Californian experience by accelerating the delivery of state services.

The state is looking to start an initial iteration of a platform that will create a digital ID and allow residents to authenticate into a centralized location and consume any of the department

services to which they are entitled. The experience needs to put people ahead of technology, keeping access easy to subscribe to, without compromising security or jeopardizing personal information. This initial platform will provide the experience between two separate state entities to prove out the benefits and set the path forward by creating a roadmap to scale and cover all state services in subsequent years at scale.

This initial effort is intended to set the state up for the future vision and establish success at the initial scale. The initial scale includes providing access across diverse a set of distinct department networks and must be seamless, giving people the impression of universal access from one session, with step up authentication when required. The proposed design will be scalable and extensible to integrate into all existing and future state digital services.

The proposed solution is for a fully integrated suite for two external online web applications between two entities. The platform will perform technology and data governance, access security, data protection, privacy, analytics, records of processing activities, and support for all types of application development tools and languages, based upon our well-regarded and familiar components.

The Digital ID effort will be architected to deliver program efficiencies and a seamless user experience for residents accessing an initial subset of state services, while prioritizing user consent and privacy, and ensuring the highest levels of security for the data involved. The ecosystem will be fully compliant with state and federal statutes and policies applicable for the type of information collected from residents for purposes of authentication, including but not limited to the Information Practices Act (IPA) and Health Insurance Portability and Accountability Privacy Act (HIPAA).

**F. Analysis of All Feasible Alternatives**

**ALTERNATIVE 1** – Approve CDT request for 2.0 positions and $1,111,000 in General Fund (GF) in Fiscal Year (FY) 2021-22 and FY 2022-23 to deploy the initial Digital ID ecosystem for a subset of state services.

PROS:

- Initiates the critical agency and department need for Digital ID with a unified ecosystem.
- Enables proactive risk identification for critical services and begins iterative improvements
- Aligns with strategic principle of putting people first, and goal of easing identification requirements across state services

CONS:

- Requires General Fund investments to make significant progress on statewide issues
- Adds CDT resources

**ALTERNATIVE 2** – Allow each agency to follow its own path. Programs and departments will be responsible for implementing, maintaining, supporting and securing multiple identity verification and authentication systems, when identity verification and authentication is a common need.

PROS:

- Small short term fiscal impact
- Maintains the current permanent staff position level at CDT

CONS:

- Multiple solutions may not result in the ultimate goal of an improved user experience and a single identifier for residents
- Some departments and agencies cannot afford to develop their own Digital ID solution
- It will be considerably more difficult to integrate a web of different solutions, or discard agency solutions later, and will be much more expensive to remediate

**ALTERNATIVE 3** – Deny the request

PROS:

- Maintains the current permanent staff position level at CDT
- No increase in General Fund spending

CONS:

- Access to services will continue to be fragmented across the State
- Will not meet the Governor's digital transformation objectives or Vision 2023 goal
- Continue state spending on individual department duplicative systems

## G. Implementation Plan

If approved, CDT will establish the positions by September 30, 2021. Once employees are onboarded, the work will commence as described in this BCP. As expert level specialists, the requested employees would engage in their designated assignments, as outlined in this BCP, on an on-going basis. The work effort will start with the identification of the target departments and state services that will be the focus of the initial deployment of the Digital ID ecosystem. The work will also provide on-going support along with development of a roadmap for Digital ID expansion across all state services.

## H. Supplemental Information

N/A

## I. Recommendation

Approve CDT request for 2.0 positions and $1,111,000 in General Fund (GF) in Fiscal Year (FY) 2021-22 and FY 2022-23 to develop and execute a scalable Digital ID ecosystem for a subset of state services.

# BCP Fiscal Detail Sheet

**BCP Title: Digital Identification** **BR Name: 7502-017-BCP-2021-AR**

## Budget Request Summary

| | CY | BY | BY+1 | BY+2 | BY+3 | BY+4 |
|---|---|---|---|---|---|---|
| | | | FY21 | | | |
| Personal Services | | | | | | |
| Positions - Permanent | 0.0 | 2.0 | 2.0 | 0.0 | 0.0 | 0.0 |
| **Total Positions** | **0.0** | **2.0** | **2.0** | **0.0** | **0.0** | **0.0** |
| Salaries and Wages | | | | | | |
| Earnings - Permanent | 0 | 239 | 239 | 0 | 0 | 0 |
| **Total Salaries and Wages** | **$0** | **$239** | **$239** | **$0** | **$0** | **$0** |
| Total Staff Benefits | 0 | 128 | 128 | 0 | 0 | 0 |
| **Total Personal Services** | **$0** | **$367** | **$367** | **$0** | **$0** | **$0** |
| Operating Expenses and Equipment | | | | | | |
| 5301 - General Expense | 0 | 2 | 2 | 0 | 0 | 0 |
| 5304 - Communications | 0 | 2 | 2 | 0 | 0 | 0 |
| 5320 - Travel: In-State | 0 | 2 | 2 | 0 | 0 | 0 |
| 5322 - Training | 0 | 2 | 2 | 0 | 0 | 0 |
| 5340 - Consulting and Professional Services - External | 0 | 500 | 500 | 0 | 0 | 0 |
| 5342 - Departmental Services | 0 | 236 | 236 | 0 | 0 | 0 |
| **Total Operating Expenses and Equipment** | **$0** | **$744** | **$744** | **$0** | **$0** | **$0** |
| **Total Budget Request** | **$0** | **$1,111** | **$1,111** | **$0** | **$0** | **$0** |

## Fund Summary

| | | | | | | |
|---|---|---|---|---|---|---|
| Fund Source - State Operations | | | | | | |
| 0001 - General Fund | 0 | 1,111 | 1,111 | 0 | 0 | 0 |
| **Total State Operations Expenditures** | **$0** | **$1,111** | **$1,111** | **$0** | **$0** | **$0** |
| **Total All Funds** | **$0** | **$1,111** | **$1,111** | **$0** | **$0** | **$0** |

## Program Summary

Program Funding

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 6230 - Department of Technology | 0 | 1,111 | 1,111 | 0 | 0 | 0 |
| **Total All Programs** | **$0** | **$1,111** | **$1,111** | **$0** | **$0** | **$0** |

**BCP Title: Digital Identification** **BR Name: 7502-017-BCP-2021-AR**

## Personal Services Details

**Salary Information**

| Positions | Min | Mid | Max | CY | BY | BY+1 | BY+2 | BY+3 | BY+4 |
|---|---|---|---|---|---|---|---|---|---|
| 1414 - Info Tech Spec II (Eff. 07-01-2021) | | | | 0.0 | 1.0 | 1.0 | 0.0 | 0.0 | 0.0 |
| 7500 - - C.E.A. - B (Eff. 07-01-2021) | | | | 0.0 | 1.0 | 1.0 | 0.0 | 0.0 | 0.0 |
| **Total Positions** | | | | **0.0** | **2.0** | **2.0** | **0.0** | **0.0** | **0.0** |

| Salaries and Wages | CY | BY | BY+1 | BY+2 | BY+3 | BY+4 |
|---|---|---|---|---|---|---|
| 1414 - Info Tech Spec II (Eff. 07-01-2021) | 0 | 103 | 103 | 0 | 0 | 0 |
| 7500 - - C.E.A. - B (Eff. 07-01-2021) | 0 | 136 | 136 | 0 | 0 | 0 |
| **Total Salaries and Wages** | **$0** | **$239** | **$239** | **$0** | **$0** | **$0** |
| Staff Benefits | | | | | | |
| 5150350 - Health Insurance | 0 | 36 | 36 | 0 | 0 | 0 |
| 5150450 - Medicare Taxation | 0 | 3 | 3 | 0 | 0 | 0 |
| 5150500 - OASDI | 0 | 15 | 15 | 0 | 0 | 0 |
| 5150600 - Retirement - General | 0 | 74 | 74 | 0 | 0 | 0 |
| **Total Staff Benefits** | **$0** | **$128** | **$128** | **$0** | **$0** | **$0** |
| **Total Personal Services** | **$0** | **$367** | **$367** | **$0** | **$0** | **$0** |