STATE OF CALIFORNIA

Budget Change Proposal - Cover Sheet

DF-46 (REV 07/23)

Fiscal Year 2024-25	**Business Unit Number** 5180	**Department** California Department of Social Services

Hyperion Budget Request Name 5180-020-BCP-2024-GB	**Relevant Program or Subprogram** Information Systems Division (ISD), Information Security, Operations

Budget Request Title
Security Architecture Compliance Assessment

Budget Request Summary
The California Department of Social Services (CDSS) requests $2,000,000 in 2024-25 to meet the new IT security Zero Trust Architecture (ZTA) and Multifactor Authentication (MFA) standards described in Statewide Administrative Manual (SAM)/ Statewide Information Management Manual (SIMM) 5360 and Cybersecurity Infrastructure Security Agency (CISA). ZTA Maturity Model requirements as defined in Technology Letter (TL) 23-01 issued by the California Department of Technology (CDT) on May 27, 2023. CDSS will engage with professional services to assess ISD's current technology environment and workforce. The outcomes of this effort will allow CDSS to understand the level of effort required to comply with the new standards. The additional resources will be used to begin CDSS's compliance activities and define the ongoing resources, technology, and time needed to meet these emerging requirements.

Requires Legislation (submit required legislation with the BCP) ☐ Trailer Bill Language ☐ Budget Bill Language ☒ N/A	**Code Section(s) to be Added/Amended/Repealed**	
Does this BCP contain information technology (IT) components? ☒ Yes ☐ No *If yes, departmental Chief Information Officer must sign.*	**Department CIO** Chad Crowe	**Date**

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

Project No. N/A **Project Approval Document:** N/A

Approval Date: **Total Project Cost:**

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 Gregory Nelson	**Date**	**Reviewed By**	**Date**
Department Director Kim Johnson	**Date**	**Agency Secretary**	**Date**

[redacted]

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

Principal Program Budget Analyst Gabrielle Santoro	**Date submitted to the Legislature** 1/10/2024

A. Problem Statement

CDSS needs professional services and support to assess its current technology environment and organizational structure to develop an effective plan to meet the new state-wide ZTA and MFA requirements. CDSS requests $2,000,000 in 2024-25 to meet these standards as described in SAM/SIMM 5360 and CISA ZTA Maturity Model requirements as defined in TL 23-01 issued by the CDT on May 27, 2023.

B. Background/History

In May 2023, the CDT introduced new requirements through Technology Letter 23-01, describing MFA and ZTA standards. These new standards are described in the SIMM 5360-C, for the implementation of SAM 5360, Identity and Access Management. TL 23-01 mandates all state entities to assess, plan and implement the initial maturity stage of the five pillars as defined by the CISA ZTA Maturity Model Version 2.0. by May 2024. This maturity model stresses that the path to zero trust is an incremental process that may take years to implement. However, zero trust will allow for more smart deployment of security efforts toward the most vital data and services in the long run, rather than "one size fits all" security investments across the whole company.

ISD provides planning and operational support, as well as information security and privacy rules and standards, application development, and support for existing and new systems. ISD manages and oversees department-wide technology activities and divisional IT projects, as well as the upkeep of state-mandated manuals and reports. ISD is also in charge of the department's enterprise architecture, technological research and analysis, and project approval document preparation guidelines.

ISD supports over 250 systems used by twelve (12) different divisions within CDSS and 58 counties, as well as other state and federal agencies, to provide services ranging from disbursement of assistance allowances and payments to in-home care providers to facilitating oversight and licensing of child and residential care facilities. These systems maintain the integrity of federal/state-mandated programs and are essential to the assessment of program performance and generating mandated reports. Many of these applications are considered mission-critical but are maintained on aging legacy platforms that are vulnerable and subject to failure.

The ISD provides a centralized IT service desk for over 5,800 CDSS employees and is responsible for support of all hardware and software associated with network PCs and laptops (clients).

ISD also provides Telecom and other services to over 4,700 customers, including CDSS employees, employees from State Council on Developmental Disabilities, the California Health and Human Services Agency, and the Office of the Patient Advocate. ISD also manages and operates the wide and local area networking infrastructure for CDSS and is responsible for installation, maintenance and refresh of servers and network equipment, and provides for recovery of data and systems in a natural or operational disaster. It provides regional office support statewide for offices throughout the State from Eureka to San Diego.

Resource History
(Dollars in thousands)

Program Budget	**PY - 4**	**PY - 3**	**PY - 2**	**PY-1**	**PY**	**CY**
Authorized Expenditures	N/A	N/A	N/A	N/A	N/A	N/A
Actual Expenditures	N/A	N/A	N/A	N/A	N/A	N/A
Revenues	N/A	N/A	N/A	N/A	N/A	N/A
Authorized Positions	N/A	N/A	N/A	N/A	N/A	N/A
Filled Positions	N/A	N/A	N/A	N/A	N/A	N/A
Vacancies	N/A	N/A	N/A	N/A	N/A	N/A

Workload History

Workload Measure	**PY - 4**	**PY - 3**	**PY - 2**	**PY-1**	**PY**	**CY**
e.g., Applications Received, Applications Processed, Call Volume, Site Visits, Audits, Stakeholder Meetings, Hearings, etc.	N/A	N/A	N/A	N/A	N/A	N/A

C. Justification

While CDSS supports ZTA implementation, it is not possible for CDSS to implement all of the policy and system changes necessary by the new standards without additional resources, technology, and assistance.

The requested funding will be used to perform and support the ZTA assessment which is crucial for CDSS to align with the new requirements set forth by the CDT. Additionally, this assessment will provide invaluable insights into the time, resources, and technology required to implement ZTA successfully within our organization. By conducting a ZTA assessment, we can evaluate our current identity and access management implementation and identify any gaps or vulnerabilities that may exist.

This assessment will enable us to address these deficiencies promptly, ensuring compliance with the new requirements and reinforcing our security posture. By proactively assessing our organization's readiness for ZTA, we can position ourselves as leaders in compliance, mitigate potential findings, and demonstrate our commitment to safeguarding sensitive information and critical infrastructure. Implementing ZTA is a complex endeavor that involves various components, such as network architecture, identity management, data protection, endpoint security, cloud security, and incident response. The ZTA assessment will provide us with a comprehensive understanding of our current state, enabling us to assess the time, resources, and technology required for successful ZTA implementation. This assessment will help us identify potential challenges, estimate costs, and develop an implementation roadmap that aligns with our organization's unique needs and priorities.

Planning for a ZTA assessment and remediation requires staff and time to address goals, objectives, scope, requirements, team roles, and responsibilities. Identifying the resources required and structuring the assessment process to support a repeatable and documented assessment provide consistency and structure.

D. Departmentwide and Statewide Considerations

This proposal is in accordance with CDSS's primary mission "to serve, aid and protect needy and vulnerable children and adults in ways that strengthen and preserve families, encourage personal responsibility and foster independence," as well as the CalHHS Agency guiding principle to cultivate a culture of innovation and deliver on outcomes.

This proposal also aligns with Cal-Secure the California Executive Branch's five-year information security maturity roadmap. Cal-Secure requires state departments including CDSS, to implement various components of ZTA. This includes implementing enhanced network access controls that limit excessive implicit trust found in traditional network security models, and Identity Lifecycle Management which can be accomplished through a secure, high-assurance identity fabric.

E. Outcomes and Accountability

The ZTA assessment for our organization aims to achieve several desired outcomes. These outcomes will serve as benchmarks for success, guiding us in strengthening our security posture and meeting the new requirements set forth by the CDT. By measuring our progress against these outcomes, we can ensure the effectiveness and value of the assessment.

Desired Outcomes:

Comprehensive Understanding of Current State:

The assessment will provide us with a holistic view of our current zero-trust posture. It will enable us to identify our strengths, weaknesses, and gaps in security architecture. This comprehensive understanding will empower us to make informed decisions and prioritize the necessary improvements to enhance our security.

Identification of Vulnerabilities and Gaps:

Through the assessment, we will identify vulnerabilities and gaps in our existing security controls and practices. This includes evaluating our network architecture, identity and access management, data protection, endpoint security, cloud security, security operations center (SOC), and incident response capabilities. By uncovering potential weaknesses, we can proactively mitigate risks and fortify our defenses.

Recommendations for Improvement:

Based on the assessment findings, the report will provide us with specific recommendations tailored to our organization's unique environment and requirements. These recommendations will outline actionable steps to strengthen our zero-trust posture and address identified gaps. The recommendations will serve as a roadmap for implementing necessary changes and improvements.

Implementation Plan:

The assessment will include a comprehensive implementation plan that details the necessary steps, timeline, resource requirements, and technology considerations for successful implementation of the recommended improvements. This plan will provide us with a clear roadmap, guiding us through the execution of changes and ensuring a seamless transition to a robust zero trust architecture.

Enhanced Security Posture:

The goal of the assessment is to significantly enhance our security posture. By implementing the recommended improvements, we aim to reduce the risk of data breaches, unauthorized access, and insider threats. Additionally, we seek to improve our incident detection and response capabilities, ensuring that our organization is better equipped to protect sensitive information, maintain business continuity, and preserve stakeholder trust.

Measurement of Success:

Improvement in Zero Trust Maturity Score:

Success will be measured by tracking the increase in our organization's zero trust maturity score. The Zero Trust Maturity Model Scorecard will assess our current maturity level and provide a baseline for comparison. As we implement the recommended improvements, we should observe measurable progress and an increase in our zero-trust maturity score.

Reduction in Identified Vulnerabilities:

Success will be measured by the reduction in the number and severity of vulnerabilities identified during the assessment. By addressing the identified gaps and vulnerabilities, we will be able to measure our success in mitigating risks and strengthening our overall security posture.

Compliance with New Requirements:

Success will be measured by our organization's compliance with the new requirements set forth by CDT, particularly regarding the implementation of Identity and Access Management (IAM). The assessment will identify any gaps in our IAM implementation, and successful compliance will demonstrate our commitment to meeting regulatory mandates.

Adoption of Recommendations:

Success will be measured by the extent to which the recommended improvements are adopted and implemented. The assessment report will provide a roadmap for implementation, and success will be determined by the timely execution of the proposed changes and enhancements.

Stakeholder Feedback and Satisfaction:

Success will be measured by stakeholder feedback and satisfaction. This includes feedback from IT leaders, executive management, and stakeholders across the organization. Positive feedback and satisfaction will indicate that the assessment has provided valuable insights and tangible improvements to our security posture.

Conclusion:

By striving for these desired outcomes and measuring our success against them, we will ensure that the ZTA assessment brings tangible value to our organization. Through a comprehensive understanding of our current state, identification of vulnerabilities and gaps, adoption of recommendations, and enhancement of our security posture, we will strengthen our resilience and align with the evolving security landscape.

Projected Outcomes

Workload Measure	CY	BY	BY+1	BY+2	BY+3	BY+4
e.g., Applications Received, Applications Processed, Call Volume, Site Visits, Audits, Stakeholder Meetings, Hearings, etc.	N/A	N/A	N/A	N/A	N/A	N/A

F. Implementation Plan

Upon approval, a competitive procurement process would begin to secure one-time professional services to perform ZTA technology environment and workforce assessment. The first year's expected schedule include the following phases:

- Initiate Competitive Procurement Process / November 2024
- Award Contract / January 2025
- Onboarding, Planning & Effort Initiation / February 2025
- Technical Assessment and Analysis / March 2025
- Workforce Analysis / July 2025
- Presentation and Alignment / September 2025

G. Supplemental Information (If Applicable)

- Technology Letter 23-01: "This TL also serves as a notice that all State entities must work toward a Zero Trust Architecture (ZTA) model as outlined in NIST 800-207. Refer to the Cybersecurity Infrastructure Security Agency (CISA) Zero Trust Maturity Model Version 2.0. By May 2024, all State agencies/entities must have assessed, planned, and implemented the "Initial" maturity stage of each of the five pillars including Identity, Devices, Networks, Applications & Workloads, and Data."

BCP Fiscal Detail Sheet

BCP Title: Security Architecture Compliance Assessment

BR Name: 5180-020-BCP-2024-GB

Budget Request Summary

Operating Expenses and Equipment

Operating Expenses and Equipment	FY24 Current Year	FY24 Budget Year	FY24 BY+1	FY24 BY+2	FY24 BY+3	FY24 BY+4
5340 - Consulting and Professional Services - External	0	2,000	0	0	0	0
Total Operating Expenses and Equipment	**$0**	**$2,000**	**$0**	**$0**	**$0**	**$0**

Total Budget Request

Total Budget Request	FY24 Current Year	FY24 Budget Year	FY24 BY+1	FY24 BY+2	FY24 BY+3	FY24 BY+4
Total Budget Request	**$0**	**$2,000**	**$0**	**$0**	**$0**	**$0**

Fund Summary

Fund Source

Fund Source	FY24 Current Year	FY24 Budget Year	FY24 BY+1	FY24 BY+2	FY24 BY+3	FY24 BY+4
State Operations - 0001 - General Fund	0	2,000	0	0	0	0
Total State Operations Expenditures	**$0**	**$2,000**	**$0**	**$0**	**$0**	**$0**
Total All Funds	**$0**	**$2,000**	**$0**	**$0**	**$0**	**$0**

Program Summary

Program Funding

Program Funding	FY24 Current Year	FY24 Budget Year	FY24 BY+1	FY24 BY+2	FY24 BY+3	FY24 BY+4
4275028 - Special Programs	0	2,000	0	0	0	0
Total All Programs	**$0**	**$2,000**	**$0**	**$0**	**$0**	**$0**