STATE OF CALIFORNIA
Budget Change Proposal - Cover Sheet
DF-46 (REV 07/23)

Fiscal Year	Business Unit Number	Department
2026-27	4120	California Emergency Medical Services Authority

Hyperion Budget Request Name	Relevant Program or Subprogram
4120-002-BCP-2026-GB	Emergency Medical Services Authority

Budget Request Title
Security Architecture Compliance Assessment

Budget Request Summary
The Emergency Medical Services Authority (EMSA) requests $250,000 one-time in 2026-27 from the General Fund to conduct initial activities to meet the Information Technology (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.

Requires Legislation (submit required legislation with the BCP)	Code Section(s) to be Added/Amended/Repealed
☐ Trailer Bill Language ☐ Budget Bill Language ☒ N/A	

Does this BCP contain information technology (IT) components? ☒ Yes ☐ No *If yes, departmental Chief Information Officer must sign.*	Department CIO Joe Sullivan	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	Date	Reviewed By	Date
Joe Sullivan	1/10/2026	Gabrielle Santoro	1/10/2026
Department Director	**Date**	**Agency Secretary**	**Date**
Elizabeth Basnett	1/10/2026	Julie Souliere	1/10/2026

[redacted]

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

Principal Program Budget Analyst	Date submitted to the Legislature
Nina Hoang	1/10/2026

A. Problem Statement

EMSA requests $250,000 in 2026-27 from the General Fund to conduct initial activities to meet the IT security ZTA and MFA standards described in SAM/SIMM 5360 and CISA.

EMSA's current communications equipment may not meet cyber security standards, such as SAM/SIMM section 5360 and 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.

In May 2023, CDT introduced new requirements through Technology Letter 23-01, describing Multifactor Authentication (MFA) and ZTA standards. These standards are described in SIMM section 5360-C, for the implementation of SAM section 5360, Identity and Access Management. TL 23-01 requires 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. Zero Trust will allow for 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 department.

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

OIT supports over 100 systems used by six different divisions within EMSA and 58 counties, as well as other state and federal agencies, to provide services ranging from Emergency Medical Services (EMS) System Development and Implementation to Disaster Medical Response and Preparedness. These systems maintain the integrity of federal and state-required programs and are necessary for assessment of program performance and generating required reports. Many of these applications are maintained on aging legacy platforms that are vulnerable and subject to failure.

OIT provides a centralized IT service desk for both EMSA and Local EMS Agency employees and is responsible for supporting all hardware and software associated with network Personal Computers and laptops (clients).

OIT also provides Telecom, radio, and satellite communication services, to both EMSA employees and California Medical Assistance Teams (CalMAT) members. CalMAT members were previously not licensed for any software or provided items such as phones, however, they are subject to requirements such as SAM section 5360 to have unique logins, including MFA functionality, to utilize state assets. OIT also manages and operates the wide and local area networking infrastructure for EMSA and is responsible for installation, maintenance and refreshing of servers and network equipment, and provides for recovery of data and systems in a natural or operational disaster. Finally, it provides field IT support during emergency medical operations.

Resource History
(Dollars in thousands)

Program Budget	2020-21	2021-22	2022-23	2023-24	2024-25	2025-26
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	2020-21	2021-22	2022-23	2023-24	2024-25	2025-26
Applications Received, Applications Processed, Call Volume, Site Visits, Audits, Stakeholder Meetings, and Hearings.	N/A	N/A	N/A	N/A	N/A	N/A

B. Justification

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

C. Departmentwide and Statewide Considerations

This proposal is in accordance with EMSA's primary mission to be responsible for "the equitable coordination, administration, and integration of the statewide emergency medical services system to reduce suffering and save lives throughout California," as well as the California Health and Human Services 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 departments, including EMSA, 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.

D. Outcomes and Accountability

The ZTA assessment for EMSA aims to achieve several desired outcomes. These outcomes will serve as benchmarks for success, strengthening security posture and taking initial steps to meet the new requirements set forth by CDT.

Desired Outcomes:

Comprehensive Understanding of Current State:

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

Identification of Vulnerabilities and Gaps:

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

Recommendations for Improvement:

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

E. Implementation Plan

Upon approval, a competitive procurement process would begin to secure professional services to perform ZTA technology environment and workforce implementation and ongoing support. The first year's expected schedule includes the following phases:

- November 2026 – January 2027: Initiate Competitive Procurement Process
- January 2027 – February 2027: Award Contract
- February 2027 – March 2027: Onboarding, Planning & Effort Initiation
- March 2027 – April 2027: Technical Assessment and Analysis
- April 2027 – May 2027: Workforce Analysis
- May 2027: Presentation and Alignment

F. Supplemental Information (If Applicable)

Fiscal Detail Sheet

BCP Fiscal Detail Sheet

BCP Title: Security Architecture Compliance Assessment

BR Name: 4120-002-BCP-2026-GB

Budget Request Summary

Operating Expenses and Equipment

Operating Expenses and Equipment	FY26 Current Year	FY27 Budget Year	FY28 BY+1	FY29 BY+2	FY30 BY+3	FY31 BY+4
5346 -Information Technology – Other	0	250	0	0	0	0
Total Operating Expenses and Equipment	**$0**	**$250**	**$0**	**$0**	**$0**	**$0**

Total Budget Request

Total Budget Request	FY26 Current Year	FY27 Budget Year	FY28 BY+1	FY29 BY+ 2	FY30 BY+3	FY31 BY+4
Total Budget Request	**$0**	**$250**	**$0**	**$0**	**$0**	**$0**

Fund Summary

Fund Source

Fund Source	FY26 Current Year	FY27 Budget Year	FY28 BY+1	FY29 BY+2	FY30 BY+3	FY31 BY+4
State Operations - 0001 - General Fund	0	250	0	0	0	0
Total State Operations Expenditures	**$0**	**$250**	**$0**	**$0**	**$0**	**$0**
Total All Funds	**$0**	**$250**	**$0**	**$0**	**$0**	**$0**

Program Summary

Program Funding

Program Funding	FY26 Current Year	FY27 Budget Year	FY28 BY+1	FY29 BY+2	FY30 BY+3	FY31 BY+4
State Operations – 0001 – General Fund	0	250	0	0	0	0
Total All Programs	**$0**	**$250**	**$0**	**$0**	**$0**	**$0**