# CEA ACTION PROPOSAL

Per California Code of Regulations, title 2, section 548.5, the following information will be posted to CalHR's Career Executive Assignment Action Proposals website for 30 calendar days when departments propose new CEA concepts or major revisions to existing CEA concepts. Presence of the department-submitted CEA Action Proposal information on CalHR's website does not indicate CalHR support for the proposal.

## A. GENERAL INFORMATION

| 1. Date | 2. Department |
|---|---|
| 2025-01-07 | Covered California |

3. Organizational Placement (Division/Branch/Office Name)

Information Technology Division’s Employee Experience, Service Delivery, Infrastructure and Operations Branch

4. CEA Position Title

Chief Technology Officer

5. Summary of proposed position description and how it relates to the program's mission or purpose. (*2-3 sentences)*

The Chief Technology Officer (CTO) leads the Information Technology (IT) Division’s Employee Experience, Service Delivery, Infrastructure and Operations Branch.  The CTO is responsible for interpreting Federal, State, and Covered California policies and regulations to develop policies and processes to secure Covered California’s strategic technology architecture, infrastructure, and digital services supporting compliant operations of our State-Based Health Benefit Exchange.

Major Responsibilities include but are not limited to: The CTO oversees the Department's technology architecture, infrastructure and digital solution delivery and operations, including the development and implementation of Covered California's security infrastructure, digital services, enterprise applications, cloud policies and strategies, and technical support enabling marketplace operations and employee productivity– all of which play a critical role in supporting the mission of Covered California.

6. Reports to: (*Class Title/Level*)

Chief Information Officer/ Exempt

7. Relationship with Department Director (*Select one)*

□ Member of department's Executive Management Team, and has frequent contact with director on a wide range of department-wide issues.

☑ Not a member of department's Executive Management Team but has frequent contact with the Executive Management Team on policy issues.

(*Explain*): Advises executive management on secure systems and infrastructure, support services including business continuity, incident management, disaster recovery policies and processes, portfolio management policy, and governance issues in a new, unique state organization.

8. Organizational Level *(Select one)*

□ 1st □ 2nd □ 3rd ☑ 4th □ 5th (mega departments only - 17,001+ allocated positions)

## B. SUMMARY OF REQUEST

### 9. What are the duties and responsibilities of the CEA position? Be specific and provide examples.

Focuses on developing secure cloud and on-premises applications and digital services, enhancing business processes, and facilitating communication among employees and contract staff in a hybrid workplace. This role serves as the principal policy maker that includes developing, implementing, and managing enterprise-wide technology policies, standards, architecture, and strategies across Covered California to support business operations and strategic objectives. The CTO is instrumental in interpreting and executing security policies that connect employers and consumers. Responsibilities include developing and maintaining the infrastructure and security operations that support the California Healthcare Eligibility, Enrollment, and Retention System (CalHEERS), CoveredCalifornia.com, and the Service Center call handling systems and operations. The CTO is tasked with ensuring the security of all platforms and databases, including:

Employee Experience:

- Develop and implement secure cloud and on-premises applications and digital services.
- Manage digital workplace policies and strategies, including business analysis and solution roadmaps.
- Oversee organizational change management, application development, configuration, testing, maintenance, and operational support.
- Implement technology debt management in compliance with Federal, State, and organizational laws, regulations, and policies.
- Adopt and incorporate responsible generative artificial intelligence (GenAI) employee-facing tools and technology based on Executive Order N-12-23 and internal Covered California GenAI policy.
- Expand Centers for Medicare and Medicaid Services (CMS) Acceptable Risk Controls for ACA, Medicaid, and Partner Entities (ARC-AMPE) information security framework across Covered California's technology solutions.
- Update the technology infrastructure and operations to adopt a Zero Trust information security framework to harden critical systems and ensure compliance with pending legislation (including California AB749, mandating Zero Trust architecture for all data, hardware, software, internal systems, and essential third-party software).

Technology Infrastructure and Operations:

- Oversee the engineering design, implementation, support, and lifecycle management of secure and highly available communications infrastructure, including network, voice, and video systems.
- Manage secure and highly available compute infrastructure, including on-premises and cloud compute and storage solutions.
- Ensure the security and high availability of end points, including desktops, laptops, tablets, and smartphones.

Technology Service Management:

- Oversee the technology service desk; facilities, A/V, and event support.
- Manage core Information Technology Service Management (ITSM) processes including problem, change, release, asset, and knowledge management.
- Handle comprehensive business continuity, disaster recovery planning, and incident response management.
- Conduct IT demand forecasting, capacity planning, and solution availability assessments.
- Implement, maintain, and evolve the IT service catalog.
- Establish and improve service quality and customer satisfaction metrics.
- Lead the Enterprise Architecture and Change Management councils.
- Make policy-level decisions on technology adoption and set Covered California standards for competing solutions.

Policies & Strategy:

- Develop, implement, and maintain enterprise-wide technology policies, standards, architecture, and strategies.
- Promote policies related to the system development lifecycle, including design, development, testing, implementation, and operations.
- Steward Covered California's Agile development methodology.
- Advise the Chief Information Officer (CIO) and executive leadership on emerging technologies, including pros and cons and solutions based on full lifecycle and cost of ownership benefit analysis.
- Make mission-critical decisions on secure, highly available infrastructure supporting Covered California's control agencies, business partners, and consumers.
- Provide technology direction and consultation to the executive leadership team, Chief Privacy Officer, IT management team, contractors, and program staff on IT policy, planning, and service delivery.
- Establish and drive efforts to influence, standardize, improve, and reuse technologies across national State-Based Exchanges.

Supervising & Administrative Responsibilities:

- Supervise and indirectly influence program administrative responsibilities, including organization design.
- Develop and manage budgets.
- Refine and model organizational culture and work practices, including normative behaviors, skills, and performance expectations.
- Manage information technology service acquisition, delivery, and lifecycle, including procurement and contract management activities.

## B. SUMMARY OF REQUEST (continued)

10. How critical is the program's mission or purpose to the department's mission as a whole? Include a description of the degree to which the program is critical to the department's mission.

☑ Program is directly related to department's primary mission and is critical to achieving the department's goals.

□ Program is indirectly related to department's primary mission.

□ Program plays a supporting role in achieving department's mission (i.e., budget, personnel, other admin functions).

Description: Covered California's mission is to increase the number of insured Californians, improve health care quality, lower costs, and reduce health disparities through an innovative, competitive marketplace that empowers consumers to choose the health plan and providers that give them the best value.

The Information Technology Division's Employee Experience, Service Delivery, Infrastructure, and Operations Branch within Covered California plays a critical role in directly supporting and advancing the overarching mission of Covered California to increase the number of insured Californians, improve healthcare quality, lower costs, and reduce health disparities.

Moreover, the implementation of secure infrastructure and systems, adherence to federal Minimum Acceptable Risk Standards for Exchanges (MARS-E), and the transition to the ARC-AMPE framework are essential in maintaining the operational integrity and security necessary for a state-based healthcare exchange. The responsibility of managing servers, networks, and cloud operations to safeguard the personally identifiable information (PII) of over 24 million residents underscores the immense trust placed in this branch. This trust extends to ensuring the security and privacy of the data of millions of Californians and all Covered California employees, a critical element in preserving the organization's credibility and reputation statewide.

The branch's commitment to adopting a Zero Trust architecture, as guided by the Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model, further solidifies its foundational role in protecting Covered California's IT assets. This proactive approach to cybersecurity is essential in an era when threats are increasingly sophisticated and pervasive.

As Covered California seeks to innovate and improve efficiency within its operations, the strategic adoption of GenAI tools for employee-facing applications is a forward-thinking move. GenAI has the potential to revolutionize how Covered California processes data and makes decisions. By integrating GenAI, the Information Technology Division's Employee Experience, Service Delivery, Infrastructure, and Operations Branch is not only enhancing operational efficiencies but also positioning Covered California at the forefront of technological innovation in healthcare. This aligns perfectly with Covered California's mission to improve healthcare quality and lower costs through innovative solutions.

The mission and purpose of the Information Technology Division's Employee Experience, Service Delivery, Infrastructure, and Operations Branch are critically integral to the department's overall mission. Without the secure, efficient, and innovative technology infrastructure and operations this branch provides, Covered California could not meet its goals of expanding coverage, improving healthcare quality, reducing costs, and minimizing health disparities. The branch ensures the operational backbone of Covered California is robust, secure, and innovative, making it fundamentally critical to the department's mission.

## B. SUMMARY OF REQUEST (continued)

11. Describe what has changed that makes this request necessary. Explain how the change justifies the current request. Be specific and provide examples.

The rapid pace of innovation in machine language (ML) and GenAI technologies is reshaping decades of technology development, implementation, and support practices. To proactively leverage these advancements (GenAI and ML) and better serve the citizens of California, Covered California is taking strategic steps to realign and enhance our organizational structure and workflow. This involves a proactive approach to adopting GenAI and ML technologies, focusing on alignment, and streamlining the responsibilities of the CTO and Deputy Chief Information Officer (DCIO) to improve service delivery.

Key organizational changes include redirecting critical enterprise architecture responsibilities from the CTO to the DCIO to consolidate capabilities and better integrate enterprise architecture with strategy and innovation. Conversely, application development responsibilities will shift from the DCIO to the CTO to achieve a modern DevOPS approach. These changes aim to enhance application development, delivery, and compliance with the evolving MARS-E and Zero Trust information security standards.

Furthermore, Covered California's strategic technology architecture, infrastructure, and digital services will be centralized under the CTO. This consolidation entails overseeing the Department's technological framework, along with the delivery and operations of digital solutions. Key responsibilities include developing and implementing Covered California's security systems, digital services, enterprise applications, and cloud-based policies and strategies. Additionally, the CTO is tasked with providing technical support, which is essential for the efficient marketplace operation and for enhancing employee productivity. Consequently, this proposal is designed to centralize the oversight of enterprise applications within our information security framework, entrusting them to the governance of a dedicated, responsible senior leader.

Additionally, the CMS, the federal oversight body for Covered California, requires all state-based healthcare exchanges to adopt ARC-AMPE, an advanced information security control framework, throughout their operations within 365 days of its release (release targeted for Fall 2024). This enhancement of the cybersecurity framework aims to cover emerging technologies, including cloud computing and employee facing GenAI. It expands ARC-AMPE compliance requirements to encompass systems that interact directly with consumers (managed by the DCIO) as well as the internal systems that manage consumer data and the technology infrastructure supporting both (managed by the CTO).

The CTO will be responsible for the secure and prudent implementation and adoption of policies across our technology portfolio, as directed by the DCIO for the integration of consumer facing GenAI within Covered California's technological offerings. Additionally, the CTO is tasked with broadening the scope of Zero Trust and MARS-E information security compliance frameworks across our entire platform, moving beyond their present application within CalHEERS.

These strategic shifts are designed to better position Covered California at the forefront of technological innovation, enabling us to deliver superior services to California's citizens while meeting stringent security and compliance standards.

## C. ROLE IN POLICY INFLUENCE

12. Provide 3-5 specific examples of policy areas over which the CEA position will be the principle policy maker. Each example should cite a policy that would have an identifiable impact. Include a description of the statewide impact of the assigned program.

The CTO will be critical in establishing, developing, and implementing new policies to develop, deliver and secure Covered California's strategic technology architecture, infrastructure, and digital services. Examples of areas which the CTO will be the principal policy maker are as follows:

o Technology Infrastructure: The CTO is designated as the principal policy maker in technology infrastructure policy. This specific policy area encompasses the development, implementation, and management of strategies to protect the technology infrastructure and operations of Covered California. This includes ensuring the security and availability of communications infrastructure (network, voice, and video), compute infrastructure (on-premises and cloud compute and storage), and endpoints (desktops, laptops, tablets, and smartphones). As the primary technology advisor, the CTO's responsibilities extend to overseeing hardware, commercial software, and cloud services, with a significant focus on technology lifecycle refresh policies and budgeting for these efforts.

An identifiable impact of the CTO's policy making in technology infrastructure is the safeguarding of sensitive health information and personal data of millions of Californians. By effectively managing and updating the technology infrastructure to prevent data breaches and technology service delivery failures, the CTO plays a critical role in maintaining the trust and reliability of Covered California's business work processes. Failure in this policy area could not only lead to significant breaches of private information but also result in substantial financial costs due to infrastructure failures and the potential for severe impacts on the statewide budget allocated for healthcare services. The statewide impact of this assigned program is, therefore, profound, as it directly influences the operational integrity of Covered California and the protection of its users' data, ensuring continuous and secure access to healthcare services across the state.

o ARC-AMPE Framework: The CTO is tasked with how the ARC-AMPE information security framework will be integrated into Covered California's suite of enterprise applications. Given that the ARC-AMPE compliance becomes mandatory 365 days after CMS' release – (release targeted for Fall 2024), adherence to this framework is required to ensure Covered California retains the ability to function as a state-based healthcare exchange. This includes securing its IRS Authority to Connect, the CMS Authority to Connect to the federal data hub, and the Authority to Operate as a state-based exchange under the Federal Patient Protection and Affordable Care Act of 2010. Failure to comply with the mandatory ARC-AMPE framework could jeopardize these authorities, thereby affecting Covered California's ability to provide seamless healthcare services and manage sensitive data securely. As such, this would directly affect public trust and stakeholder confidence in Covered California's reliability and security protocols.

o AB 749 - CISA Zero Trust Maturity Model: The CTO is responsible for interpreting legislation and developing operational policies and procedures to implement a Zero Trust architecture in line with the CISA Zero Trust Maturity Model. Although AB 749 is not mandated yet (legislation has not yet passed out of the legislature), Covered California is proactively embracing three key components of this framework to protect its IT assets. These components include:

- Multifactor Authentication (MFA): The implementation of MFA across all systems significantly boosts data and system security, significantly reducing the risk of unauthorized access and the security breaches.
- Enterprise Endpoint Detection and Response (EDR): Implementing EDR solutions to promote real-time detection of cybersecurity threats and enable rapid investigation and remediation, minimizing operational disruptions.
- Robust Logging Practices: Establishing logging practices that provide adequate data to support security investigations and proactive threat hunting. This proactive approach ensures the integrity of data management and maintains public and stakeholder trust in Covered California's security protocols.

Each policy area requires a strategic vision and a commitment to data security, ensuring that millions of Californian's sensitive data entrusted to Covered California is safe and secure.

## C. ROLE IN POLICY INFLUENCE (continued)

13. What is the CEA position's scope and nature of decision-making authority?

The CTO holds significant decision-making authority, primarily concentrated on the organization's technology landscape, encompassing both operational technology frameworks and security measures. Covered California is statutorily exempt from the oversight of the California Department of Technology (CDT), granting the CTO comprehensive responsibility in policy development, oversight, and the delivery of technology solutions. This includes steering the strategic technology direction in alignment with federal, state, and organizational policies, ensuring a compliant and efficient operation of the State-Based Health Benefit Exchange. The CTO's role is critical in adopting unbiased, fair, equitable, and responsible GenAI solutions to boost the capabilities and productivity of Covered California’s staff.

Further responsibilities involve directing the technology service management functions crucial for business continuity, disaster recovery planning, and incident response management, as well as overseeing IT demand forecasting and capacity planning. The CTO is responsible for developing and implementing enterprise-wide technology policies, standards, and strategies, making key policy-level decisions on technology adoption that align with Covered California’s strategic goals. This role also encompasses leadership and management of technical staff, contractors, and vendors, including talent management, budgetary responsibilities, and fostering an organizational culture of innovation and productivity. Additionally, ensuring strict compliance with legal and regulatory requirements, like the implementation of a Zero Trust architecture, is a significant part of the CTO’s role, securing Covered California's technology infrastructure across network, voice, video, computing, and mobile devices, which are essential for the organization's operations. Through this extensive scope of responsibilities, the CTO is instrumental in shaping Covered California's technological future, securing the effective delivery of digital services, and supporting the organization's mission.

14. Will the CEA position be developing and implementing new policy, or interpreting and implementing existing policy? How?

The CTO will develop and implement new policies, as well as interpret and implement existing policies which directly impact the following IT areas: Client Technologies and Employee Solutions.

The CTO is crucial in navigating the complexities of aligning technology infrastructure and digital solutions with both Federal and State regulations. By leading efforts in the Information Technology Division’s Employee Experience, Service Delivery, Infrastructure, and Operations Branch, the CTO ensures the secure and compliant operation of the strategic technology architecture, infrastructure, and digital services. This includes overseeing policies throughout the system development lifecycle, which are essential for supporting Covered California's operations and strategic goals while safeguarding consumer and employee information.

Additionally, the CTO is tasked with interpreting CMS’ new ARC-AMPE information security framework, applying it across the entire Covered California enterprise to comply with CMS and IRS rules governing the secure operations of an ACA-compliant state-based healthcare exchange. This role extends to interpreting and implementing solutions in support of the Governor’s Executive Order N-12-23, which mandates the proactive adoption of GenAI technologies to enhance the delivery of the agency's mission.

The CTO will develop policy and implement systems infrastructure and operations adhering to a zero-trust information security framework in alignment with best practices for operating critical technology infrastructure and pending legislation (AB749). The CTO's responsibilities, therefore, encompass a broad spectrum of policy engagement, from crafting new directives that respond to emerging technological and regulatory landscapes, to adapting and enforcing existing policies to uphold Covered California’s commitment to providing accessible, high-quality healthcare coverage.