

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

06/19/26

2. Department

California Department of Public Health

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

Information Technology Services Division

4. CEA Position Title

Assistant Deputy Director, Chief Artificial Intelligence and Security Operations Officer (CAISOO)

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

The proposed CAISOO Career Executive Appointment (CEA) B position provides executive leadership over Artificial Intelligence (AI), Machine Learning (ML), Generative AI (GenAI) initiatives, cybersecurity operations, identity and access management, and enterprise solutions architecture—functions that are foundational to the secure and innovative delivery of public health services. This role directly supports the California Department of Public Health's (CDPH) mission of enhancing the well-being of California's diverse people and communities by ensuring that emerging technologies are ethically governed, securely implemented, and strategically aligned with statewide public health objectives.

6. Reports to: (Class Title/Level)

Deputy Director, Information Technology Services Division/Chief Information Officer, CEA C

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*):

The CAISOO serves as a senior executive advisor to the Directorate, providing strategic leadership and expert counsel on the responsible adoption and governance of AI across the enterprise. In this capacity, the CAISOO plays a pivotal role in aligning AI initiatives with the state's broader digital transformation goals, ensuring that innovation is grounded in sound principles of data architecture, secure system design, and operational integrity.

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.

The CEA will serve as the executive leader responsible for the strategic direction, policy development, and operational oversight of four critical technology domains that support CDPH's public health mission:

1. AI/ML/GenAI Functions and Initiatives

Lead the integration of AI, ML, and GenAI into public health systems through strategic planning, innovation, and research to improve outcomes and advance health equity. Oversee AI/ML project life cycle management, policy development for ethical and transparent use, and staff training to build internal capabilities. Represent CDPH in inter-agency collaborations to align AI strategies with state and federal priorities and guidelines. Drive digital transformation by implementing governance frameworks, enhancing enterprise services, expanding data access, and promoting agile, reusable solutions for sustainable operations. Act as a change leader to communicate technology vision, foster a culture of innovation, and ensure projects align with customer needs and strategic goals.

2. Security Operations

Maintain and advance CDPH's cybersecurity strategy through a robust framework that safeguards systems and data while enabling secure operations. Develop readiness strategies for emerging GenAI and quantum threats, including post-quantum cryptography. Lead SOC incident response for rapid threat mitigation and promote a strong security culture through department-wide training and awareness programs. Align public health strategies with state priorities such as: Departmental Strategic Plans to address the objective of strengthening foundational public health and health care infrastructure at the state and local levels by leveraging data technology to advance goals and inform action and accountability around the enhancement of surveillance systems, leveraging data and technology for greater decision intelligence, and strengthening the science base for services; California Office of Health Equity Portrait of Promise to address clear and persistent health disparities linked to social and historical inequities as part of a multi-pronged public health effort to achieve health equity for all Californians; California Health and Human Services Agency (CalHHS) guiding principles to advance data-driven and person-centered services and supports statewide efforts to address the health needs of our most vulnerable communities and populations; California Department of Technology (CDT) Vision 2023, to use technology to meet society's goals, and make progress on large scale, complex problems affecting Californians all into 2023 and beyond; and supporting CDT's vision for a government that is accessible and reliable, as well as leveraging public health information to make CDPH more efficient and effective, and make public health data more accessible and reliable.

3. Identity and Access Management (IAM)

Define and enforce access control policies that ensure only authorized users can access sensitive systems and data. Oversee the deployment and maintenance of secure authentication and authorization systems. Manage onboarding and offboarding processes to ensure accurate and timely access rights. Conduct regular audits to detect and respond to unauthorized access or anomalies. Lead the implementation of major transformation initiatives and efforts that execute the strategies and items on enterprise road maps, while ensuring the implementation continues to have a focus on strengthening ties with programs, local health departments and community stakeholders.

4. Solutions Architecture

Lead the design and implementation of scalable, secure IT systems to support CDPH programs, ensuring rapid, secure data sharing and seamless integration of new technologies. Establish architectural standards for consistency and compliance, manage vendor relationships, and modernize legacy infrastructure for agility, interoperability, and sustainability. Drive technology innovation and cloud-based modernization to enable efficient public health operations, streamlined systems, and rapid data services. Collaborate with the ITSD Chief Technology Officer (CTO) and program leadership to enhance data interoperability, improve asset management, and promote information sharing for timely, accurate public health insights.

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: The CAISOO CEA position will serve as a cornerstone of CDPH's strategic and operational capacity. This role directly supports the CDPH mission of enhancing the well-being of California's diverse people and communities by ensuring that emerging technologies are ethically governed, securely implemented, and strategically aligned with statewide public health objectives. This executive role is entrusted with leading the Department's most advanced and security-sensitive technological domains, including AI, ML, GenAI, Security Operations, IAM, and Enterprise Solutions Architecture.

Mission-Critical Functions

- 1. Enabling Data-Driven Public Health Innovation**
The position is responsible for the strategic planning, implementation, and oversight of AI/ML/GenAI initiatives that directly enhance CDPH's ability to analyze, predict, and respond to public health challenges. These technologies are essential for modernizing disease surveillance, improving health equity, and accelerating decision-making across the Department's programs.
- 2. Safeguarding Public Health Infrastructure**
Through comprehensive leadership of Security Operations, the role ensures the confidentiality, integrity, and availability of CDPH's information systems. This includes preparing for emerging threats such as GenAI-based attacks and quantum computing vulnerabilities, which are critical to maintaining public trust and operational continuity.
- 3. Ensuring Secure and Compliant Access to Health Systems**
By overseeing IAM functions, the position guarantees that access to sensitive health data is tightly controlled, auditable, and aligned with state and federal compliance requirements. This is vital for protecting patient privacy and enabling secure interagency collaboration.
- 4. Architecting Scalable and Interoperable Public Health Systems**
The CEA leads the design and integration of enterprise IT solutions that support the Department's evolving public health initiatives. This includes ensuring secure data sharing, aligning with architectural best practices, and enabling rapid deployment of new technologies to meet urgent health needs.
- 5. Degree of Criticality**
This position is indispensable to the Department's ability to fulfill its public health mission. It operates at the nexus of innovation, security, and infrastructure—domains that are foundational to the Department's effectiveness in protecting and promoting the health of Californians. The role's influence spans strategic leadership, operational execution, and policy development, making it a mission-critical asset to the Department's present and future success.

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 creation of this new CEA position is driven by significant programmatic, legislative, and policy changes that have expanded the scope and complexity of CDPH's technology integration responsibilities. Recent statewide initiatives, including the Regulatory Lean Process Improvement and mandates for IT legislative bill analysis integration, require a leadership role with authority to shape policy and governance across multiple programs. These changes are not incremental. They represent a fundamental shift in how CDPH aligns with evolving state laws, Governor's Office directives, and internal compliance frameworks.

1. Emergence of AI/ML/GenAI in Public Health

The integration of AI, ML, and GenAI into public health operations has moved from exploratory to essential. These technologies now underpin critical functions such as disease surveillance, predictive modeling, and real-time decision support. The Department must have executive-level oversight to strategically plan and govern AI/ML/GenAI initiatives, ensure ethical and equitable deployment of these technologies, and align with federal and state partners on shared AI frameworks and standards.

2. Escalating Cybersecurity Threats

The public health sector has become a prime target for sophisticated cyber threats, including those enabled by GenAI and emerging quantum computing capabilities. The Department must proactively defend against these risks by implementing post-quantum cryptographic strategies, leading a mature technically focused security operations center, ensuring rapid incident response and continuous threat monitoring.

3. Increased Complexity in Identity and Access Management

As CDPH expands its digital footprint and interconnectivity with external partners, the need for robust IAM has intensified. This includes enforcing granular access controls to protect sensitive health data, managing user provisioning across a growing ecosystem of systems and stakeholders, conducting continuous audits to ensure compliance and mitigate insider threats.

4. Demand for Scalable, Inter-operable Solutions Architecture

Public health initiatives now require agile, scalable, and secure IT architectures that can support rapid deployment, data sharing, and cross-agency collaboration. This role is essential to design and implement enterprise-grade solutions aligned with public health goals, integrate emerging technologies without disrupting legacy systems, and establish architectural standards that promote sustainability and innovation.

Budgetary investments further underscore this need. For example, the implementation of a unified public health services platform is projected to save ~\$900,000 in FY 2025-26 and up to \$10.1 million annually in licensing costs over time. This initiative demands executive-level oversight to ensure cost savings are realized while maintaining service continuity and compliance.

Impacted Programs and Stakeholders:

-Collaboration with Local Health Jurisdictions (LHJs) will require CDPH adopt new data-sharing protocols, governance and security standards as part of statewide modernization efforts.

-Data sharing with and across CalHHS Departments, such as the Department of Health Care Services (DHCS) and Department of Social Services (DSS), will require coordinated IT policy alignment for integrated health data systems.

-Programmatic work surrounding Immunization, Chronic Disease Prevention, and Emergency Preparedness is constantly experiencing changes in service delivery models and compliance requirements that will be further complicated with the adoption of AI and GenAI tools and systems modernization.

-External vendors and contracted service providers will need to comply with new security and interoperability standards and meet reference architectures developed and maintained by CDPH.

These changes and expansion in CDPH's role necessitate new policy frameworks and updates to existing responsibilities, particularly in areas such as AI, cybersecurity, data governance, and legislative compliance. The CEA will act as the principal policy maker within the defined domains, ensuring statewide consistency, accountability, and strategic alignment. Without this role, CDPH risks delays in modernizing and implementing critical programs and meeting statutory obligations. The convergence of advanced technologies, heightened security demands, and the evolving nature of public health delivery necessitates a dedicated executive to lead these domains. This position is not only justified—it is imperative to ensure that CDPH can continue to protect and promote the health of Californians in an increasingly digital and threat-prone environment.

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.

1. AI/ML Governance

Policy Example: Development and enforcement of a statewide AI/ML Governance Framework for public health applications.

Description: This policy would establish ethical, legal, and operational standards for the use of AI/ML technologies across CDPH programs, including disease surveillance, predictive analytics, and resource allocation.

Statewide Impact: Ensures consistent, equitable, and transparent use of AI/ML technologies across all public health programs, reducing bias in health outcomes and improving the speed and accuracy of public health interventions.

2. GenAI Use and Risk Mitigation

Policy Example: Implementation of a Responsible GenAI Use Policy for internal and external public health communications and decision support.

Description: This policy would define acceptable use cases, data governance requirements, and human oversight protocols for GenAI tools used in public health messaging, diagnostics, and administrative automation.

Statewide Impact: Protects the integrity of public health information, mitigates misinformation risks, and ensures that GenAI tools enhance rather than compromise public trust and decision-making.

3. Post-Quantum Cryptography and Cybersecurity Resilience

Policy Example: Adoption of a Post-Quantum Cryptography Transition Plan for all CDPH systems handling sensitive health data.

Description: This policy would guide the phased implementation of quantum-resistant encryption standards to protect against future cryptographic threats.

Statewide Impact: Strengthens the long-term security of California's public health infrastructure, ensuring continuity of operations and protection of personal health information in the face of emerging cyber threats.

4. IAM Standards

Policy Example: Establishment of a Statewide IAM Policy for Public Health Systems.

Description: This policy would define role-based access controls, multi-factor authentication requirements, and life cycle management protocols for all users accessing CDPH systems.

Statewide Impact: Enhances data security and operational efficiency across all CDPH programs by ensuring that only authorized personnel can access sensitive systems and information.

5. Enterprise Solutions Architecture and Interoperability

Policy Example: Creation of a Public Health Systems Architecture and Integration Policy.

Description: This policy would standardize architectural principles, data exchange protocols, and vendor integration requirements for all new and existing public health IT systems.

Statewide Impact: Promotes interoperability, scalability, and cost-efficiency across California's public health technology ecosystem, enabling faster deployment of services and better coordination during emergencies.

Each of these policy areas reflects a critical intersection of technology and public health, and the proposed executive role is uniquely positioned to lead their development and implementation. The statewide impact of these policies would be profound - enhancing security, equity, innovation, and resilience across California's public health infrastructure.

C. ROLE IN POLICY INFLUENCE (continued)

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

This CEA position would hold broad and strategic decision-making authority across multiple mission-critical domains within CDPH. This authority spans policy development, operational oversight, interagency coordination, and enterprise-level technology governance. The position functions with a high degree of autonomy and accountability, consistent with the expectations of executive leadership roles in state government.

1. Policy Formulation and Strategic Direction

The CEA serves as the principal architect of policies governing the ethical, secure, and effective use of emerging technologies including AI, ML, and GenAI within the Department. This includes establishing statewide standards for AI/ML deployment in public health programs, defining ethical frameworks and compliance protocols for GenAI use, and leading the Department's alignment with federal and state technology strategies. These decisions directly shape how CDPH leverages innovation to improve health outcomes, manage risk, and ensure equity in service delivery.

2. Operational Oversight and Risk Management

The position exercises executive authority over the Department's SOC, with responsibility for directing incident response strategies, implementing post-quantum cryptographic protections, and managing enterprise-wide security awareness and readiness programs. These decisions have immediate and long-term implications for the integrity of CDPH's information systems and the protection of sensitive health data statewide.

3. Enterprise Identity and Access Governance

The CEA is empowered to define and enforce IAM policies that govern user authentication, authorization, and provisioning across all CDPH systems. This includes approving access control frameworks, overseeing audit and compliance mechanisms, and ensuring secure interagency and partner access to public health systems. These decisions are foundational to maintaining trust, privacy, and operational continuity across the Department's digital infrastructure.

4. Technology Architecture and Investment Decisions

The position has authority to design and approve enterprise IT architectures that support CDPH's evolving public health mission. This includes selecting and integrating scalable, secure technologies, establishing architectural standards and best practices, managing vendor relationships and technology procurement strategies. These decisions directly impact the Department's ability to deploy responsive, interoperable, and cost-effective public health solutions across California.

The CEA's decision-making authority is both strategic and operational in nature, encompassing the full life-cycle of technology policy, implementation, and oversight. The position is empowered to make high-impact decisions that affect not only internal CDPH operations but also the broader public health ecosystem across the state. Its scope reflects the complexity and urgency of modern public health challenges, and its authority is essential to ensuring that CDPH remains secure, innovative, and mission-aligned in a rapidly evolving technological landscape.

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

The CEA's authority spans both the creation of new policy in uncharted technological areas and interpretation and implementation of existing regulatory frameworks. This dual responsibility ensures that CDPH remains both innovative and compliant—able to lead in emerging domains while upholding the trust and legal obligations expected of a public health agency. The proposed CEA position will be responsible for developing and implementing new policy, as well as interpreting and implementing existing policy. This dual function is essential due to the rapidly evolving nature of the technologies under the position's purview and the increasing complexity of public health operations.

Developing and Implementing New Policy

The CEA will serve as the principal policy architect for emerging domains where no comprehensive state-level policy currently exists. This includes AI/ML/GenAI Governance: The position will lead the creation of new policies that define ethical use, transparency standards, and operational protocols for artificial intelligence and machine learning in public health programs. These policies will guide how predictive models are used in disease surveillance, resource allocation, and public communication. Post-Quantum Cryptography Readiness: As quantum computing advances, the CEA will be responsible for developing forward-looking policies that transition CDPH systems to quantum-resistant encryption standards. This includes establishing timelines, risk thresholds, and compliance benchmarks. Enterprise Architecture Standards: The CEA will define new architectural frameworks and integration policies to ensure that CDPH's IT infrastructure is scalable, secure, and interoperable with external partners and state systems.

Interpreting and Implementing Existing Policy

The CEA will interpret and apply existing federal and state policies to ensure CDPH's compliance and alignment with broader public sector mandates. The CEA will operationalize existing laws such as HIPAA, California's Information Practices Act, and statewide cybersecurity directives by translating them into actionable security strategies, incident response protocols, and access control mechanisms. The position will interpret state procurement policies and standards (e.g., SAM/SIMM guidelines) to guide the selection and integration of third-party technologies and services. The CEA will ensure that CDPH's data sharing practices comply with existing memoranda of understanding, legal agreements, and statewide interoperability frameworks.