

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

2019-12-01

2. Department

California Earthquake Authority

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

Information Technology Department

4. CEA Position Title

Chief Information Officer

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

The California Earthquake Authority (Authority) proposes to upgrade the Assistant Chief Information Officer (C.E.A. Level A) to Chief Information Officer (C.E.A. Level B) due to the major changes in duties and responsibilities. The proposed Chief Information Officer will initiate the strategic development and direct the governance of Information Technology activities within the Authority including all Information Technology projects and initiatives, purchases, and contracts to ensure conformity with the Authority's Enterprise Architecture. This position will develop, modify, and oversee the implementation of policies, long-range goals, work plans, and strategies related to meeting the Information Technology needs of the Authority and its client groups, in addition advising the Authority's Chief Executive Officer, the Governing Board and executive team in IT policies and procedures to support the business development and requirement of the Authority.

6. Reports to: (Class Title/Level)

Chief Executive Officer / ("At Will" Contract Employee)

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):

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 C.E.A Level B, Chief Information Officer (CIO) directs and manages the Authority's computing and information-technology strategic plans, policies, programs, and schedules for its business- and finance-data processing, technical infrastructure, computer services, network communications, and management-information services.

As a member of the Executive Staff, the CIO participates directly in setting and implementing policies that affect the Authority and its 25 Participating Insurers (PIs). The CIO advises the Executive Staff and the Governing Board on all policy decisions affecting IT operations, services, enterprise-wide applications, infrastructure that integrates to and supports on the business needs and routine operations of the Authority. This includes but is not limited to:

- Develop and execute the IT security strategies and structure required to protect and mitigate the risks to the Authority's data, intellectual property (IP), and assets.
- Determine, establish, and maintain the IT services and security framework and policies to align the Authority's IT with the Authority's business goals and strategies.
- Establish, measure, and report IT Key Performance Indicators (KPIs).
- Determine, direct, recruit, and maintain the IT resources required to successfully meet approved the Authority's business needs.
- Initiate and implement new policies and revise existing policies necessary to enforce enterprise-wide policies related to IT operations, IT services, IT Security, project approval, multiple application systems, IT procurement and vendors management, enterprise architecture, and accessibility while ensuring alignment with the Authority's IT strategic goals.

The CIO establishes and executes strategies to optimize the use of existing IT assets and resources; develops, maintains and reports the Authority's IT annual budget and purchases including:

- Justifications of all IT budget items.
- Policies and procedures of IT budget and procurement management.
- Return on Investment (ROI) of IT budget items.
- Total IT estimated costs of proposed and approved initiatives and projects including the planned vs. actual costs of completed work.

The CIO participates in the Governing Board meetings to present and report the IT status, and advise the Governing Board members on the Authority's IT polices and strategies. The CIO ensures information and data integrity across all information technology functions, and acting from an executive position, monitors and validates the Authority's compliance with security policies and regulatory requirements applicable.

**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 Authority is California's not-for-profit provider of residential earthquake insurance - privately funded and publicly managed, with programs to encourage and support effective action to reduce the risk of earthquake damage and loss. The department's vision is to promote and support long-term family and community resilience by providing risk education, loss mitigation, and insurance protection to help Californians prepare for and recover from damaging earthquakes.

The CIO directs the IT initiatives and efforts to support the Authority's routine operations, disaster-recovery, governance, change-management, information security and privacy, IT policies and procedures, and portfolio and project management. For instance, the IT department has provided information technology platforms and services which enable the Participating Insurers to sell the products and report to the Authority through the IT mediums. Currently, the Authority has access to personally identifiable information (PII) for over one million Californians, and over \$17,000,000,000 in claim payment capacity.

The Authority's IT programs are directly related to and support the Authority's mission and vision, and ensure the Authority's ongoing service to the policyholders and public is accessible, prompt and effective.

## 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 Authority is a not-for-profit insurance company established by the California legislature in 1996. The Authority is the largest residential earthquake insurer in the country and one of the largest in the world.

Since its inception in late 1996, the Authority's IT platform and infrastructure have consistently and significantly evolved as the company has grown and as technology has changed. The Authority started with 14 participating insurers accounting for about 2,200 policies, and IT works were almost fully outsourced. In 2012, the Authority began developing software internally to support the Authority's needs. In 2013, a contract Chief Insurance & Technology Officer (CITO) was hired to oversee the Insurance & Technology Department, which consists of three functions including Insurance & Claims, Insurance Education & Sales Support (IESS), and Information Technology (IT) Division. The Assistant Chief Information Officer (C.E.A - Level A) position was established in 2017 to manage the Information Technology(IT) Branch under the general direction of the CITO.

In the beginning of 2019, the Authority obtained necessary approval to reorganize the Insurance & Technology Department. The Information Technology (IT) function was split from the previous Insurance & Technology Department and became an independent IT Department, which provides all IT-related services to the Authority. In the meantime, the contract CITO position was removed, and the Assistant Chief Information Officer was assigned in an acting capacity as the "Chief Information Officer", who independently manages the new-established IT Department, and oversees the full IT functions that support the business operation of the Authority and its various programs.

With the expansion of the duties and responsibilities, the Authority requests to upgrade the current Assistant Chief Information Officer position (C.E.A Level A) to the Chief Information Officer (C.E.A Level B) to reflect the major changes in duties and responsibilities. In the CIO capacity, the incumbent assumes the full spectrum of duties related to IT strategic planning, IT operational management, policies making, and program and project management. Specifically, the CIO performs the following duties and responsibilities that were previously performed by the CITO :

- The Authority's IT program management and planning - Direct the IT Department moving from a software development focus to a solution provider focus, in order to meet the new and current business needs of the Authority.
- Policy making and enhancement - Direct and manage the Authority's IT strategic plans, policies and schedules for its business- and finance-data processing, establish IT policies and processes requiring all IT solutions to consider the use of existing IT assets as a first option.
- Resources Management - Align IT resources and skill sets to maximize the understanding and implementation of existing assets. Establish end-to-end IT costs that include assets, resources, and annual maintenance to be used when calculating return on investment. Establish a resource plan and adjust IT organization structure to align with the solution provider focus that includes required skill sets.
- Relationship Management - manage the Authority's relationships with its counterparts employed by the Authority's participating insurers and key IT vendors, carry out those duties in accordance with the requirements of the Authority's Governing statues and regulations, and under the lawfully exercised authority of the Authority's Governing Board.
- As an Executive staff, participates in the Authority's governing board meeting and makes formal presentation as required, communicates the Authority's IT policies to all internal and external stakeholders to ensure the Authority's goals and objectives are related accurately.

### 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 CIO develops, maintains, and implements all Information Technology (IT) strategic and operational planning for the Authority, and acts as the principle policy maker to ensure all the new or existing policies and procedures are consistent with the Authority's mission, goals and business strategies.

The CIO initiates and implements new policies, revises existing policies, and enforces all enterprise-wide policies related to IT operations, services, security, and development, including the procurement and management of outside resources and services. The CIO ensures that the policies associated with enterprise architecture, accessibility, oversight and management align with the Authority's IT strategic business goals.

The CIO establishes, executes and maintains the strategies and processes to maximize the value of IT solutions and services to staff and customers, including engagement, analysis, development and implementation of IT and the Authority long-range goals, plans and strategies. The CIO develops the policies necessary to develop and maintain a governance framework and the associated metrics to be applied to the implementation of new technologies and systems, including data access, storage, backup, privacy, and disaster recovery and/or business continuity. The CIO also supervises and works with the CISO and managers in IT Department to set policies, standards and procedures about how information security is managed throughout the Authority.

For instance, the CIO plans and directs the development of the Authority's IT strategic plan, policies, programs and schedules in order to achieve and improve business operations; fosters innovations, aligns IT with the Authority's business strategy, prioritize IT initiatives, and coordinate the evaluation, deployment, and management of current and future IT systems across the Authority. In addition, the CIO oversees the Authority's information security program which includes the risk mitigation, assessment and protection of all information assets. Develops policies and procedures to ensure information and data integrity, security, privacy, and compliance across all IT platforms and functions. From an executive-management position, monitors and validates the Authority's compliance with security policies and regulatory requirements. Directs the necessary IT initiatives to support disaster-recovery, business continuity, governance, change management, security, compliance, and privacy. Directs the development and implementation of IT policies, processes, and controls. Directs and manages the IT portfolio and associated projects. Develops the metrics and key performance indicators (KPIs) necessary to measure the performance of IT and its procedures and processes. Directs IT business process improvements. Oversees the delivery of reporting and metric management processes to enable the effective evaluation of IT services. Communicates the Authority's IT policies to all internal and external stakeholders to ensure the Authority's goals and objectives are related accurately. As a member of Executive Staff, participates in the Authority's Governing Board meeting and makes formal presentation as required. Promotes positive, cooperative, professional work relations among staff and peers of diverse workforce to facilitate an effective workplace free of discrimination and harassment.

**C. ROLE IN POLICY INFLUENCE (continued)**

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

The CIO directly reports to the Chief Executive Officer and serves as a member of the Authority's executive-management team. As the Executive in the IT Department, the CIO oversees the whole IT Department within the Authority, directs and manages the Authority's computing and information-technology strategic plans, programs, and schedules for its business- and finance-data processing, computer services, network communications, and management-information services. The CIO also reports to the Authority's Governing Board as required.

The CIO exercises full decision making authority for all IT functions including but not limited to: IT policies, governance and metrics, IT security and compliance, information and data integrity, budget, contracting, procurement and vendor management, IT services and help desk, IT infrastructure, enterprise-wide IT programs and projects, and IT personnel management and staffing needs, etc.

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

The CIO identifies and develops new policies, revise existing policies necessary, and enforces enterprise-wide policies related to IT operations, IT services, IT Security, project approval, various application systems, IT procurement and vendors management, enterprise architecture, accessibility, and oversight while ensuring alignment with the Authority's IT strategic goals. For example, the CIO develops and implements the enterprise data management policy to regulate how the data is shared between business units; develops and executes the IT security strategies and structure required to protect and mitigate the risks to the Authority's data, intellectual property (IP), and assets.