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: 2026-01-12

2. Department: California Earthquake Authority

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

Risk and Actuarial Department

4. CEA Position Title

Chief Information Security Officer (CISO)

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) is requesting approval to establish the CISO position within the Risk and Actuarial Department as a Career Executive Assignment (CEA) Level A. The proposed CISO will oversee and direct all of the Authority's information security initiatives and work efforts, develop and implement all of the enterprise policies and strategies pertaining to information security, and play a crucial role in advising internal and external stakeholders with the processes and requirement of the organization's security policies.

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

Chief Risk and Actuarial 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*): Directly communicates with Chief Risk and Actuarial Officer, Chief Administrative Officer (CAO), Chief Executive Officer (CEO), and Chief Finance Officer (CFO) to determine information security needs and programs that significantly impact the operation and effectiveness of the Authority.

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 Authority's CISO is responsible for managing risks related to information security and compliance regulations, as well as the implementation and maintenance of all enterprise policies and strategies associated with the security of the Authority's electronic data. The Authority data includes personally identifiable information (PII) from over 3,000,000 current and past California policyholders and the financial data required to manage claim payment capacity in the multi-billions. The CISO is also accountable for and directs the planning and execution of all the Authority's information security initiatives and work efforts including:

- the development, approval, implementation, and execution of the Authority Information Security Strategic Plan
- the development, approval, and maintenance of the Authority Information Security Risk Assessment including the prioritization of the identified risks
- the development, approval, implementation, and execution of the Authority Information Security Risk Management Program, including vendor risk management and the assessment and treatment of risks that may result from partners, consultants, and other service providers
- the development, approval, implementation, and execution of the Authority Information Security projects and work plans including associated schedules and milestones
- the development, approval, implementation, and execution of the Authority Information Security Annual Budget
- the development, approval, and maintenance of the Authority Information Security Compliance Program

On a recurring basis, the CISO will report to the Executive staff and Governing Board the status of information security, including:

- the current state of information security
- risks associated with the current state
- recommendations to mitigate current risks
- the status of the implementation and execution of the Authority Information Security Strategic Plan including project or work plan impediments and mitigation recommendations

Additionally, the CISO will be responsible for:

- anticipating new security threats and staying current with evolving infrastructures and threat strategies
- ensuring required security and controls are in place and operating effectively to maintain SOC 2, Type II certification
- integrating application development security into the Authority Software Development Lifecycle (SDLC)
- developing the appropriate policies and strategies to handle security incidents and coordinate investigative activities including incident response development, implementation, training, and execution
- acting as a focal point for the Authority’s information security investigations and, when necessary, direct a full investigation with recommended courses of action
- ensuring that disaster recovery and business continuity plans are in place and tested on a recurring schedule
- developing and implementing information security education programs to raise user awareness and security compliance
- continuing education and professional certification to remain current on emerging information security vulnerabilities

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 core mission of the Authority is to manage the financial aspects and risks associated with managing two multi-billion-dollar insurance funds using effective risk transfer programs, as well as promoting community resilience through education, loss mitigation, and insurance protection.

The information platforms and systems utilized by the Authority not only enable routine organizational operations and management, including access to sensitive financial and claim paying information, but also provide access to PII of over three million California policy holders. As such, it is essential the maintenance and security of this sensitive data is protected. The CISO plays an integral role in supporting the mission of the CEA and provides oversight into departmental functions specific to these safeguards, including:

Security and Controls – Leads information security and governance throughout the Authority, which includes defining and advising on information security strategies and managing data protection efforts, establishing and implementing organizational policies, processes, and audit controls, and developing and delivering ongoing security training.

Monitoring and Reporting – Maintains oversight and provides direction on all information security issues or incidents, including testing incident response processes, monitoring alerts, identifying potential threats, and implementing effective security solutions.

Comprehensive Information Security Strategy – Works collaboratively with all Authority departments to identify business objectives, security risks, and compliance requirements to establish data security safeguards, appropriate information sharing processes, and coordination of incident responses.

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.

As a not-for-profit insurance company established by the California legislature in 1995-1996, the Authority is the largest residential earthquake insurer in the country and one of the largest in the world. In addition to the insurance function of financing repair and rebuilding should a catastrophic earthquake occur in California, the Authority also educates and financially helps residents strengthen their homes to reduce the impact and cost of earthquake losses. Although not an agency or department of the California government, as a public instrumentality the Authority is governed by a Board composed of five elected public officials, including California's Governor, Treasurer, and Insurance Commission.

Since its inception in 1996, the Authority has grown to cover more than 60% of the residential earthquake insurance market which includes the additional private insurers that have come on board as Authority participants. Today, the CEA has over 20 participating insurers and covers nearly one million residences throughout California, with about $19 billion in claim-paying capacity and more than $900 million in annual premium revenue. Although the Authority is publicly managed, its business purpose is comparable to that of a private-sector residential property insurance company and maintains access to sensitive PII on current and past California policyholders. Additionally, since 2019, the Authority has administered the California Wildfire Fund with assets of nearly $13 billion under management.

This means recruitment and retention of qualified, highly skilled, private-sector insurance professionals is critical to the success of Authority's mission, operations, and ongoing evolution. The California Earthquake Authority Act (CEA Act) authorizes the Authority's Governing Board to contract with, and hire, individuals with that specialized talent and significant private-sector insurance experience. As the Authority evolved and stakeholders developed a better understanding of the skills, talent, and staff size needed to run a statewide insurance operation, the Governing Board supported the Authority's leadership in hiring numerous temporary staff members at all levels (including professional) to enable the organization to successfully fulfill its mission.

This position was previously established and the duties were being performed by an authorized contract employee. This request is being submitted to re-establish this role as a civil service, CEA level position.

Appointing a CISO at the CEA level will allow the organization to continue developing and implementing the Authority's information security policies and strategic plan, including budget, for the advancement and deployment of information security technologies, identity and access management program enhancement, and integration of appropriate system security policies and information protection strategies. This will require an executive-level position be available to oversee all information security processes and procedures, coordinate the internal and external efforts to integrate appropriate system security policies, and inspire confidence and trust through strong policies and procedures regarding security of electronic information. To ensure that these new functions are adequately conducted, a CISO at the CEA level is needed to load share the vast amount of ongoing and new mission critical work.

Additionally, the CISO role is vital in advancing the Authority’s compliance with California Governor’s Executive Orders related to digital transformation, cybersecurity enhancements, and responsible adoption of emerging technologies. Notably, as Generative Artificial Intelligence (AI) technologies become integral to government operations, the CISO will guide the safe, ethical, and strategic integration of AI tools within the organization, ensuring these innovations support mission objectives while addressing data security and governance concerns.

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 CISO plays a crucial role in shaping and maintaining the organization's information security roadmap and framework, which includes significant responsibilities in the following policy development:

Governance, Policy, and Training: The CISO will develop and implement high-level policy to ensure the procedures and tools provide for the integrity and security of the infrastructure, and information for the Authority and partners are in place. These policies are not merely procedural—they are strategic instruments that safeguard data, ensure compliance with state and federal mandates, and promote responsible use of technology. The CISO ensures personnel, contractors, systems, and assets operate within a unified policy framework.

Furthermore, the CISO establishes and enforces the structures that guide decision-making, risk management, and performance monitoring. Through rigorous governance, the CISO guarantees the Authority's security operations are transparent, ethical, and aligned with statewide standards. Security administration, consulting, and oversight are all part of this governance framework, reinforcing the Authority's commitment to integrity and excellence. In each of these areas—governance, policy, and training—the CISO contributes the highest level of technical expertise, business acumen, and strategic foresight.

Threat Detection and Response: The CISO is responsible for leading and providing oversight to any information security issues that requires a response, such as security incidents. This includes maintaining and monitoring the alerts or indications of potential security incidents from any system within the organization's technology environment. Effective incident response requires close coordination between both Information Security and IT throughout the response lifecycle. The CISO is responsible for establishing a security incident response process that incorporates key personnel at all stages as appropriate. Additionally, the CISO is responsible for testing the security incident response process in partnership with IT and key stakeholders from other business units on an annual basis at a minimum.

Risk and Vulnerability Management for Information Security: The CISO will develop, implement, and enforce of the Authority Information Security Risk Management Program, including vendor risk management and the assessment and treatment of risks that may result from partners, consultants, and other service providers. This program and associated policies will establish security standards, strengthen cybersecurity posture, reduce risk of data breaches, ensure enterprise compliance, and support public trust in the systems that house sensitive and financial data for a million-plus Californians.

Identity and Access Management: The CISO will ensure the Authority has an Identity and Access Management (IAM) framework that is compliant with applicable laws and regulations and manages risks effectively. This framework includes developing processes, policies, and standards for IAM. The CISO is also responsible for ensuring sufficient IAM technology solutions are implemented that facilitate the management of electronic identities to reduce the risk of internal and external data breaches.

C. ROLE IN POLICY INFLUENCE (continued)

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

The CISO position's scope of decision-making authority is broad. The decisions made by the incumbent in this position have a significant impact to the Authority, partners, and stakeholders. The CISO is the second-level support responsible for information security and control activities within the Authority. The CISO provides consultation and advices to the Chief Risk and Actuarial Officer regarding security policies and governance, risk and threat management, IT infrastructure improvement, and access management.

The CISO will be responsible for establishing, implementing, and enforcing new policies, as well as revising existing policies necessary for the Authority's information security operations, project approval, telecommunication systems, procurement, enterprise architecture, accessibility, and oversight while ensuring alignment with the Authority's strategic goals, and protect the organization's assets, network, and data security.

In addition, the CISO will exercise broad independence of action under the Authority's strategic plan. The CISO has formal authority to make policy recommendations and is expected to proactively identify risks, operational challenges, and opportunities for innovation. The CISO will provide the Chief Risk and Actuarial Officer and the Executive Team ongoing strategic advice and operational accountability for the full scope of security concerns, policy development, training initiatives, costs versus benefits, emerging threats, new technology initiatives, and will work in conjunction with executives, management staff, and information security professionals in establishing policies that affect the security of the Authority, Participating Insurers, and California homeowners.

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

The CISO will play a strategic leadership role in developing and implementing new policy, as well as interpreting and enforcing existing policy. One of the essential functions of this position is to monitor the Authority's security vulnerabilities, threats, and events; conduct audits and comprehensive risk assessments; and develop and implement new security policies, metrics, and procedures. The evolution of technology will continually require the CISO to develop and revise policies that can support the Authority's critical business, insurance, education, and mitigation programs. The CISO will be responsible for initiating and implementing necessary new policies and revising existing policies related to information security and safety, to ensure the successful implementation and alignment with legislative mandates, state governance frameworks, and the Authority's strategic goals.