

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

5/2/2018

2. Department

California Earthquake Authority

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

Insurance and Technology 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 (the Authority) is requesting approval to establish the CISO for the Insurance and Technology Department at the Career Executive Assignment (CEA) Level. This proposed CISO will oversee and direct all of the Authority's IT security initiatives and work efforts, develop and implement all of the enterprise policies and strategies pertaining to IT security, be involved in a broad range of Information Technology activities within the department, and advise the Authority's Chief Insurance and Technology Officer (CITO), and executive team.

6. Reports to: (Class Title/Level)

Chief Insurance and Technology Officer (CITO) / ("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 CITO, Chief Operation Officer (COO), Chief Executive Officer (CEO), and Chief Finance Officer (CFO) to determine IT 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 the development, implementation, and maintenance of all enterprise policies and strategies associated with the security of CEA electronic data. CEA data includes personally identifiable information (PII) from over 1,000,000 CEA policy holders and the financial data required to manage the over \$14,000,000,000 of claim payment capacity. The CISO is also accountable for and directs the planning and execution of all of the Authority's IT security initiatives and work efforts including:

- the development, approval, implementation, and execution of the CEA Information Security Strategic Plan
- the development, approval, and maintenance of the CEA Information Security Risk Assessment including the prioritization of the identified risks
- the development, approval, implementation, and execution of the CEA Information Security Risk Management Program that includes 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 CEA Information Security projects and work plans including associated schedules and milestones
- the development, approval, implementation, and execution of the CEA Information Security Annual Budget
- the development, approval, and maintenance of the CEA Information Security Compliance Program

On a recurring basis, the CISO will report to the CEA Executive staff and CEA 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 CEA Information Security Strategic Plan including project or work plan impediments and mitigation recommendations

Additionally, the CISO will be responsible for:

- anticipating new security threats
- staying current with evolving infrastructures and threat strategies
- integrating application development security into the CEA 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 IT 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 technology has been integrated with the Authority's processes, I&T department in the Authority supports not only insurance and technology functions, but also the Authority's routine operations and management. The I&T department provides information technology platforms and systems which enable the Participating Insurers (PIs) to sell the products and reports to the Authority through the IT mediums. Currently, the Authority has access to personally identifiable information (PII) for over 1,000,000 policy holders, and over \$14,000,000,000 in claim payment capacity. The safety and security of IT systems is essential to protect the sensitive data and information of the over 1 million Californians insured and the related \$14B in insurance funds.

In addition, I&T department also supports the Authority to educate, mitigate and insurance Californians about their earthquake risk, which is directly associated with the primary mission of the Authority. In accordance with the Authority's Strategic Plan 2017 ~ 2019, technology is the primary tool to effectively present the Authority's information to policyholders and the public, promote innovative residential earthquake-loss-mitigation measures, and implement and continuously improve the Authority's insurance solutions. Therefore, the program has been significantly influencing the operations and effectiveness of the Authority.

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 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: California's Governor, Treasurer, and Insurance Commissioner serve as voting members of this Governing Board, while the Speaker of the Assembly and the President Pro-Tempore of the Senate serve as non-voting members.

Since its inception in 1996, the Authority has grown to cover more than 80% of the residential earthquake insurance market which includes the additional private insurers that have come on board as Authority participants. Over the past decade its assets have grown from \$2 billion to almost \$5 billion, and its claim-paying capacity increased over 40 percent to more than \$10 billion. With some 840,000 policies in force throughout California, the Authority each year now writes well over \$500 million in premium.

Although the Authority is publicly managed, its business purpose is comparable to that of a private-sector residential-property-insurance company. This means the organization requires professional insurance expertise on-staff to fulfill its mission. In fact, recruitment and retention of qualified, highly skilled, private-sector insurance professionals is critical to the success of Authority's operations and ongoing evolution. The California Earthquake Authority Act (CEA Act) authorizes the Authority's Governing Board to contract with, and hire, that specialized talent-the present Authority roster contains seven individuals with significant private-sector insurance experience, recruited and hired in this manner.

By law, the Authority also employs civil servants. The original CEA Act restricted the number of civil service employees the organization could employ, stating, "employees subject to civil service provisions shall not exceed 25." 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-starting some 12 years ago-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.

The primary reason for a CISO at the CEA level is the result of the dramatic up-tick in responsibility and the need for developing and implementing the Authority's IT security policies and strategic plan, including budget, for the deployment of information security technologies and program enhancement that include identity and access management, and integration of the Authority's IT systems development with the appropriate security policies and information protection strategies. This will require that an executive-level position be available to oversee the development and implementation of security policies and procedures, coordinate the internal and external efforts to integrate the current and future IT systems with appropriate security policies, and inspire confidence and trust in information technology through strong policies and procedures regarding privacy and 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.

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 will develop and implement high-level policy to ensure the procedures and tools that can provide for the integrity and security of the IT infrastructure and information for the Authority and partners are in place. These high-level policies cover risk management, identity and access management, vulnerability management, threat management, etc. The CISO will collaborate with key stakeholders to establish an IT security risk management program, which includes vendor risk management and the assessment and treatment of risks that may result from or impact our Participating Insurers, vendors, partners, consultants, and other service providers.

The Authority currently has IT assets on premise, within a vendor managed data center, Microsoft Azure Cloud, Amazon AWS S3 Cloud, Heartland Business Systems multi-tenant cloud and Insuresoft Diamond systems. The Authority is aligned with the best practices and standards of the insurance industry. As such, the Authority has begun moving the majority of its IT assets into the Azure environment. This effort is scheduled to be complete by the year of 2019. The CISO will be required to collaborate with the cloud provider, vendor data centers, and internal IT team to develop, plan, and implement IT security programs and policies to ensure that the department has implemented the hardware and software elements to provide the necessary information security infrastructure used by the Authority and its partners. The CISO will also coordinate with other departments within the Authority to ensure standards of application development security and physical security are in alignment with industry standards and best practices.

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 IT security and service activities within the Authority. The CISO provides consultation and advices to the CITO regarding IT security policies and procedures, risk and threat management, IT infrastructure improvement, and privacy and access management, etc.

The CISO will be responsible for establishing and implementing new policies and revising existing policies necessary to enforce the Authority's policies related to IT operations, IT services, IT Security, project approval, telecommunication systems, procurement, enterprise architecture, accessibility, and oversight while ensuring alignment with the Authority's IT strategic goals, and protect the Authority's IT assets, network and data security, and privacy. The scope covers the Authority's business office, vendor data centers, IT and network infrastructure, Microsoft Azure Cloud, Amazon AWS S3 Cloud, Heartland Business Systems multi-tenant cloud and Insuresoft Diamond systems.

In addition, the CISO will exercise broad independence of action under the Authority's strategic plan and oversight, and The CISO will advise the CITO and the Executive Team on all policy decisions affecting physical and IT security for the Authority, will work in conjunction with executives and management staff, and information security professional organizations in establishing policies that affect the security of the Authority, PIs and California homeowners.

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

The CISO will develop and implement new policy, and interpret and implement 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 and implement new security policies, metrics, and procedures. The evolution of technology will continually require the CISO to develop and revise IT policies that can support the Authority's critical business, insurance, education and mitigation programs. The CISO will be responsible for initiating and implementing new policies and revising existing policies necessary related to IT security and safety, to ensure the successful implementation and alignment with the Authority's strategic goals.