

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

01/04/2017

2. Department

State Compensation Insurance Fund

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

Risk Management/Enterprise Security

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)

Under the general direction of the Chief Risk Officer, the CISO provides leadership, management direction and policy guidance to State Fund's Enterprise Security Office. The CISO plans, organizes and directs activities associated with the following enterprise-wide information security programs: Security Oversight Committee, Vulnerability Assessment, Risk Assessment, Security Architecture, Incident Management, Automated Security Processes, Audit Compliance, Policy Compliance, Computer Investigation, and Business Continuity. The CISO develops, implements, and maintains policies, standards, procedures, and guidelines for information security management to ensure the security, confidentiality, integrity, availability, and privacy of State Fund's information assets. The CISO serves as an expert policy advisor to the Chief Executive Officer (CEO), and the Executive Committee.

6. Reports to: (Class Title/Level)

Chief Risk 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): The CISO serves as an advisor to the CEO.

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.

Under the general direction of the Chief Risk Officer, the CISO provides leadership, management direction and policy guidance to State Fund's Enterprise Security Office. The CISO plans, organizes and directs activities associated with the following enterprise-wide information security programs: Security Oversight Committee, Vulnerability Assessment, Risk Assessment, Security Architecture, Incident Management, Automated Security Processes, Audit Compliance, Policy Compliance, Computer Investigation, and Business Continuity. The CISO develops, implements, and maintains policies, standards, procedures, and guidelines for information security management to ensure the security, confidentiality, integrity, availability, and privacy of State Fund's information assets. The CISO serves as an expert policy advisor to the Board, Chief Executive Officer (CEO), the Executive Committee (EC), and Risk Management.

Provides leadership, management and policy direction for the work activities and performance of Enterprise Security. Plans, directs and organizes the work of staff responsible for Security Oversight Committee, Vulnerability Assessment, Risk Assessment, Security Architecture, Incident Management, Automated Security Processes, Audit Compliance, Policy Compliance, Computer Investigation, and Business Continuity. Facilitates information security governance and oversees the development and implementation of information security strategies and architecture. Oversees the planning and implementation of complex hardware and software systems, applications, and interfaces and assesses the impact of new technology on security. Oversees the planning and coordination of security incident investigation and responses and the investigation of security needs. Oversees the research and evaluation of new information security technology necessary to fortify State Fund's security profile.

Develops, implements and maintains policies and technical security standards that improve State Fund's cyber security position and protects the confidentiality, integrity, availability of systems, networks, and information assets. Ensures State Fund's information security programs and policies meet requirements of authoritative and regulatory bodies. Formulates and directs the development and implementation of new or revised policy and procedures necessitated by legislative, policy and/or information system changes. Monitors the external threat environment for emerging threats and advises relevant stakeholders on the appropriate courses of action. Continually assesses information security programs for operational risks and vulnerabilities and develop and implements robust risk mitigation strategies and strengthens cybersecurity controls. Develops and oversees performance management and metrics to track progress, measure outcomes, and validate the effectiveness of mitigation activities.

Collaborates with the Chief Technology Officer on security and risk issues. Advises and consults on matters related to business continuity and the mitigation of business disruption. Participates with Risk Management in threat analysis. Acts as a policy advisor to the Board, CEO, EC and Risk Management.

Participates in board meetings and delivers formal written and oral presentations. Act as an internal technical advisor, provides briefings, continuing education and expert consultation and advice in rendering sensitive operational and risk mitigation decisions. Reports potential and emerging program risks. Designs, develops and conducts annual security assessments and report findings and remedial actions to the CEO/EC. Represents State Fund and serves as the direct interface with the California Department of Technology's Information Security Office. Represents State Fund before constituent groups, State agencies and the legislature. Maintains relationships with internal and external stakeholders to advance State Fund's commitment to the protection of its information assets.

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 program area under the direction of the CEA is responsible for enterprise-wide information security in support of State Fund's purpose of providing fairly priced workers' compensation insurance, helping make workplaces safe, and restoring injured workers. State Fund has an investment portfolio of \$18.5 billion in investment assets (as of December 31, 2015). For over 100 years, State Fund has served California's strong, stable, fairly priced workers' compensation insurance provider as mandated by the State constitution.

Information is a valuable asset to be protected from unauthorized access, inspection, use, disclosure or modification. State Fund is committed to protecting the confidentiality, integrity, and availability of the information assets of the Department and its members and does so via its dedicated Enterprise Security. The CISO will develop, implement, and maintain enterprise policies, standards, procedures, and guidelines for information security management to ensure the security, confidentiality, integrity, availability, and privacy of State Fund's information assets.

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.

In recognition of the continued growth and operational complexity of State Fund programs, and the need to develop, fortify and implement more robust information security strategies and respond to the rapidly evolving cyber threat environment, State Fund management has assessed Enterprise Security's organizational structure and is establishing a new senior leadership position titled Chief Information Security Officer. This position will report to the Chief Risk Officer and will be an expert advisor to the CEO, the EC and Risk Management on all matters relating to information security, cyber threat prevention, protection and response. The CISO will be charged with identifying and implementing information security risk management strategies and activities to improve State Fund's security posture and ensure that State Fund's technology and information remains secure against the constantly changing landscape of security threats.

State Fund is tasked to pro actively, but prudently keep abreast and address the ever-evolving environment and issues it operates within. This requires keeping pace with an evolving threat landscape. Information security is one of the top risks to the organization as State Fund would suffer severe financial and reputational risk as a consequence of inadvertent, unauthorized, or malicious disclosure of confidential and/or sensitive information or a systems breach resulting in business disruption. Since the delivery of services and the State Fund's \$18.5 billion portfolio depend on the reliability and credibility of data and systems, there is pressing need to increase focus on improving critical security infrastructure and mature Enterprise Security. An information security breach could have a significant impact threatening business viability.

State Fund is required to comply with California's data security statute and data breach notification law. California continues to strengthen and tighten regulations around data security to ensure that businesses and state agencies establish reasonable security procedures that protect California residents' personal information. Most recently, California enacted A.B. 1541 effective January 2016, which expanded the definition of "personal information" under California's data security statute. This bill revises the definition of personal information to include defined health insurance information, and a username or email address combined with a password or security question and answer for access to an on-line account. This amendment brings the definition of personal information in the data security statute into harmony with California's data breach notification law. As California enacts new data security legislation, State Fund will need to review and revise data security and data breach notification policies and procedures to ensure legal compliance.

As cyber threat actors develop more sophisticated cyber intrusions, there is necessity for more sophisticated information security strategies critical to protecting the confidentiality, integrity and availability of the information assets of State Fund. This requires a high level Senior Leadership position to lead, manage and direct the development of robust cyber threat defenses.

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.

State Fund conducts and is responsible for its own information security operations in-house. The CISO will be responsible for the strategic direction, policy development and management of the State Fund information security architecture and supporting infrastructure critical to managing investments and the delivery of services. The CISO will oversee and provide policy direction for the following information security programs:

- Security Oversight Committee
- Vulnerability Assessment
- Risk Assessment
- Security Architecture
- Incident Management
- Automated Security Processes
- Audit Compliance
- Policy Compliance
- Computer Investigation
- Business Continuity

As an expert advisor to the organization, the CISO develops, recommends and implements information security policies, strategies and initiatives in support of State Fund's Strategic Plan, annual business plan, risk management, and fiduciary responsibility. Enterprise Security manages risk by:

- Establishing information security policies to ensure security requirements, controls and responsibilities are defined.
- Providing oversight of users, systems and networks to ensure compliance with the Information Security policy, standards and procedures as well as industry best practice.
- Monitoring networks and computers to identify possible security breaches, which include both intrusions and misuse.
- Providing high-level expertise in the discipline of computer and network security, vulnerability assessment, virus detection, and hacking methodologies.
- Conducting an annual security assessment, and reporting findings and remedial actions to the Board, the CEO and the EC.
- Developing and implementing security awareness education and establishing training guidelines for State Fund staff.

New policies and standards are continuously required as technology advances. State Fund cannot afford to be complacent since cyber criminals are constantly inventing new tools and techniques and are getting better at identifying gaps and unknown vulnerabilities in an organization's security.

C. ROLE IN POLICY INFLUENCE (continued)

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

The CISO will direct the development and implementation of policies for all Information Security programs and operations that will safeguard State Fund's information assets. The CISO will plan, organize and direct the work of professional staff responsible for enterprise-wide security programs. The CISO will serve as a policy advisor to the Board, the CEO, the EC and Risk Management, providing briefings, continuing education, and expert consultation and advice in rendering sensitive operational and risk mitigation decisions. The CISO will have influence and policy discretion to improve and strengthen State Fund's internal governance processes providing centralized decision making and coordination of all State Fund information security activities to responsibly manage risk to the organization. As a member of State Fund's Senior Leadership Team, the CISO will participate in program and policy direction.

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

State Fund conducts an annual assessment including assessing State Fund's strengths, weaknesses, opportunities, and threats, potential legislative changes, and current and future projects that impact the system's long-term sustainability. The CEA will formulate and direct the development of new or revised information security policies and strategies based on this assessment. Additionally, each year State Fund's business plan is fine-tuned to represent the focus of the organization allowing State Fund to continually assess the changing environment including regulatory changes, operational risks, and financial market risks. The CEA will formulate and direct the development of new or revised information security policies and strategies based on these ongoing challenges to ensure continued commitment to protecting the confidentiality, integrity and availability of the information assets.