

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

04/12/2016

2. Department

California State Teachers' Retirement System (CalSTRS)

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

Office of the General Counsel / Information Security Office

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 General Counsel, the Chief Information Security Officer (CISO) provides leadership, management direction and policy guidance to CalSTRS Information Security Office. The incumbent plans, organizes and directs activities associated with the following enterprise-wide information security programs: Security Architecture, Risk Management, Compliance, Threat Detection, Incident Response, Investigations, Projects & Analysis, and Operations. The CISO develops, implements, and maintains enterprise policies, standards, procedures, and guidelines for information security management to ensure the security, confidentiality, integrity, availability, and privacy of CalSTRS information assets. The incumbent serves as an expert policy advisor to the Chief Executive Officer (CEO), Executive Staff, the Teachers' Retirement Board (TRB) and its Audits & Risk Management (ARM) Committee related to these responsibilities.

6. Reports to: (Class Title/Level)

General Counsel (Statutory Position - per education code 22212.5)

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): As a member of Senior Leadership, serves as an expert policy advisor and resource to CEO, General Counsel, Executive Staff, the Teachers Retirement Board and its Audits & Risk Management Committee.

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 General Counsel, the Chief Information Security Officer (CISO) provides leadership, management direction and policy guidance to CalSTRS Information Security Office. The incumbent plans, organizes and directs activities associated with the following enterprise-wide information security programs: Security Architecture, Risk Management, Compliance, Threat Detection, Incident Response, Investigations, Projects & Analysis, and Operations. The CISO develops, implements, and maintains enterprise policies, standards, procedures, and guidelines for information security management to ensure the security, confidentiality, integrity, availability, and privacy of CalSTRS information assets. The incumbent serves as an expert policy advisor to the Chief Executive Officer (CEO), Executive Staff, the Teachers' Retirement Board (TRB) and its Audits & Risk Management (ARM) Committee related to these responsibilities.

\* Provide leadership, management and policy direction for the work activities and performance of the Information Security Office. Plan, direct and organize the work of staff responsible for Information Security Architecture, Risk Management, Compliance, Threat Detection, Incident Response, Investigations, Projects & Analysis, and Operations. Facilitate information security governance and oversee the development and implementation of information security strategies and architecture. Oversee the planning and implementation of complex hardware and software systems, applications, and interfaces and assess the impact of new technology on security. Oversee the planning and coordination of security incident investigation and responses and the investigation of security needs. Oversee the research and evaluation of new information security technology necessary to fortify CalSTRS security posture.

\*Develop, implement and maintain policies and technical security standards that improve CalSTRS cyber security posture and protect the confidentiality, integrity, and availability of CalSTRS systems, networks, and information assets. Ensure CalSTRS information security programs and policies meet requirements of authoritative and regulatory bodies. Formulate and direct the development and implementation of new or revised policy and procedures necessitated by legislative, policy and/or information system changes. Monitor the external threat environment for emerging threats and advise relevant stakeholders on the appropriate courses of action. Continually assess information security programs for operational risks and vulnerabilities and develop and implement robust risk mitigation strategies and strengthen cybersecurity controls. Develop and oversee performance management and metrics to track progress, measure outcomes, and validate the effectiveness of mitigation activities.

\*Serve as a member of CalSTRS Architecture Standards Council, Project Review Council, Enterprise Information Management Council and Risk Management Roundtable. Serve as a Senior Leadership representative on other CalSTRS governance councils and organization-wide forums. Collaborate with the Chief Technology Officer on security and risk issues. Advise and consult on matters related to business continuity and the mitigation of business disruption. Participate in CalSTRS SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis which assists the TRB in evaluating the organization's current strategic position and identifies potential threats to the organization. Promote information security awareness and oversee the design, development, and establishment of information security awareness education that inform employees about their information security privacy protection responsibilities.

\*Act as a policy advisor to the CEO, Executive Staff, the TRB and its ARM Committee recommending and implementing policies and strategies in support of the TRB's Strategic Plan, Annual Business Plan, risk management, and fiduciary responsibility. Participate in board meetings and deliver formal written and oral presentations. Act as an internal technical advisor to the ARM Committee providing briefings, continuing education and expert consultation and advice in rendering sensitive operational and risk mitigation decisions. Report potential and emerging program risks to the Committee. Design, develop and conduct annual security assessments and report findings and remedial actions to the ARM Committee. Represent CalSTRS and serve as the direct interface with the California Department of Technology's Information Security Office.

\*Represent CalSTRS before constituent groups, State agencies and the legislature. Maintain relationships with internal and external stakeholders to advance CalSTRS 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 CalSTRS mission to secure the financial future and sustain the trust of California's educators.

CalSTRS is the largest educator-only pension fund in the world with an investment portfolio of over \$186.1 billion in investment assets (as of December 31, 2015). CalSTRS administers a hybrid retirement system as part of a comprehensive financial security package for members, consisting of traditional defined benefit, cash balance and voluntary defined contribution plans, as well as disability and survivor benefits. For over 100 years, CalSTRS has served California's public school educators and their families, who today number 895,956 from the state's 1,700 school districts, county offices of education and community college districts.

Information is a valuable asset to be protected from unauthorized access, inspection, use, disclosure or modification. CalSTRS is committed to protecting the confidentiality, integrity, and availability of the information assets of CalSTRS and its members and does so via its dedicated Information Security Office. The Chief Information Security Officer 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 CalSTRS information assets. The incumbent will serve as an expert policy advisor to the Chief Executive Officer (CEO), Executive Staff, the Teachers' Retirement Board (TRB) and its Audits & Risk Management (ARM) Committee related to these responsibilities. The CEA will oversee activities that monitor and evaluate conditions in the internal and external environments and the ongoing potential risk of cyber-terrorism or computer hacking that would result in information security, financial, operational and or reputational loss to CalSTRS. Because CalSTRS services depend on the reliability and credibility of data and systems, information security is an essential risk management function. Inadequate information security risk management would have a significant impact on the delivery of member benefits (approximately \$12 billion annually) and the investment of CalSTRS \$186.1 billion portfolio.

## 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 CalSTRS programs, and the need to develop, fortify and implement more robust information security strategies and respond to the rapidly evolving cyber threat environment, the General Counsel has assessed the Information Security Office's organizational structure and is establishing a new senior leadership position titled, Chief Information Security Officer. This position will report to the General Counsel and will be an expert advisor to the CEO, Executive Staff, the TRB and its Audits & Risk Management (ARM) Committee on all matters relating to information security, cyber threat prevention, protection and response. Under the oversight of the ARM Committee and CalSTRS General Counsel, the Chief Information Security Officer will be charged with identifying and implementing information security risk management strategies and activities to improve CalSTRS' security posture and ensure that CalSTRS' technology and information remains secure against the constantly changing landscape of cybersecurity threats.

CalSTRS 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 cyber threat landscape. The TRB has identified information security as one of the top risks to the organization as CalSTRS 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 member services and the investment of CalSTRS \$186.1 billion portfolio depend on the reliability and credibility of data and systems, there is pressing need to increase focus on improving critical cybersecurity infrastructure and mature the Information Security Office.

Each year CalSTRS conducts environmental scan activities including assessing CalSTRS strengths, weaknesses, opportunities, and threats (SWOT), potential legislative changes, and current and future projects that impact the system's long-term sustainability. Of significant concern to the TRB are the financial and operational risks that may hinder CalSTRS long-term sustainability and operational efficiency. The SWOT analysis revealed threats of increased risk exposure due to ongoing potential risk of cyber-terrorism or computer hacking resulting in high potential for information security, financial, operational and/or reputational loss. The SWOT analysis also revealed a weakness that the maturation of the Information Security Office processes and procedures are progressing, but are not yet complete. CalSTRS staff review and update an enterprise Risk Management Report internally on a quarterly basis with biannual reports to the TRB. The Risk Management Report ranks the category of Information Security as a high risk. The report emphasizes the need to mitigate risks in the event of loss of information security or compliance violations as a result of unauthorized or unintentional breaches which pose potential risk of not being able to provide mission critical business processes to our members. The report identifies the impact of an information security breach as "Major" as a security breach could have a significant impact threatening business viability.

Importantly, CalSTRS is currently focused on efforts to replace its current pension administration system which tracks, monitors, calculates benefits, records and reports retirement data throughout the educator's and beneficiary's lifetime. This effort is known as Pension Solution and will be one of CalSTRS largest and riskiest projects of which CalSTRS has embarked. CalSTRS has budgeted over \$219 million dollars for this effort. The pension administration technology conversion requires the preparation of a smooth transition that preserves the confidence of stakeholders, customers and employees. To mitigate and avoid the risks associated with such a large, multi-year, complex, and costly pension system replacement thorough planning is critical. The CISO will have a key senior leadership role on the Pension Solution Team charged with identifying and mitigating information security risks associated with this high risk project.

CalSTRS 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, CalSTRS 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 CalSTRS and its members. This requires a high level Senior Leadership position to lead, manage and direct the development of robust cyber threat defenses. As the largest educator-only pension fund in the world it is imperative that CalSTRS has the appropriate management, oversight, and enterprise focus of all information security strategies and activities.

### 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.

CalSTRS independently conducts its information security operations, as these efforts are independent of typical state oversight by the Department of Finance, the Department of General Services and the California Technology Agency. This independence and autonomy comes with a significant amount of management risk. CalSTRS squarely assumes full responsibility and accountability for success or failure of its information security strategies and programs. In the context of CalSTRS status as the largest teacher public pension system in the world, this assumption of risk is essentially unprecedented in state government. CalSTRS operates primarily apart from the state control functions and is under the oversight of the Teachers' Retirement Board (TRB); as such, CalSTRS conducts and is responsible for its information security operations in-house. CalSTRS CISO will be responsible for the strategic direction, policy development and management of the CalSTRS information security architecture and supporting infrastructure critical to managing investments and the delivery of pension benefits and services. The CISO will oversee and provide policy direction for the following information security programs:

- Security Architecture
- Risk Management
- Compliance
- Threat Detection
- Incident Response
- Investigations

As an expert advisor to the CEO, Executive Staff, TRB and its Audits & Risk Management Committee (ARM), the CISO develops, recommends and implements information security policies, strategies and initiatives in support of CalSTRS Strategic Plan, annual business plan, risk management, and fiduciary responsibility. The Information Security Office manages risk by:

- Establishing information security policies to ensure security requirements, controls and responsibilities are defined.
- Providing oversight of CalSTRS users, systems and networks to ensure compliance with the CalSTRS 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 TRB's ARM Committee.
- Developing and implementing security awareness education and establishing training guidelines for CalSTRS staff.

New policies and standards are continuously required as technology advances. CalSTRS 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.

The statewide impact of these policies impact 1,005 internal users, 895,956 public school educators and their families, and the state's 1,700 school districts, county offices of education and community college districts.

**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 CalSTRS information assets. The CISO will plan, organize and direct the work of professional staff responsible for the following programs: Security Architecture, Risk Management, Compliance, Threat Detection, Incident Response, Investigations, Projects & Analysis, and Operations. The CISO will formulate forward thinking information security strategies and enhancements with a focus on CalSTRS long-term sustainability.

The CISO will serve as a policy advisor to the the CEO, Executive Staff, the TRB and its Audits & Risk Management (ARM) Committee. As the highest information security expert, the CISO will serve as an internal expert and technical advisor to the ARM Committee providing briefings, continuing education, and expert consultation and advice in rendering sensitive operational and risk mitigation decisions. The incumbent will have influence and policy discretion to improve and strengthen CalSTRS internal governance processes providing centralized decision making and coordination of all CalSTRS information security activities to responsibly manage risk to the organization.

As a member of CalSTRS Senior Leadership team, the CISO will participate in program and policy direction. The CISO will be a member of CalSTRS Architectural Standards Council, Project Review Council, Enterprise Information Management Council, Risk Management Roundtable, and will also serve as a Senior Leadership representative on multiple organization-wide forums.

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

Each year CalSTRS conducts environmental scan activities including assessing CalSTRS strengths, weaknesses, opportunities, and threats (SWOT), potential legislative changes, and current and future projects that impact the system's long-term sustainability. Each year, the TRB is presented with an analysis of the organization's strengths and weaknesses of the internal organization as well as the external opportunities and threats that might impact CalSTRS in a positive or negative way. The CEA will formulate and direct the development of new or revised information security policies and strategies based on this analysis. Additionally, each year CalSTRS business plan is fine-tuned to represent the focus of the organization allowing CalSTRS to continually assess the changing environment including regulatory changes, operational risks, financial market risks and the changing needs of CalSTRS members. The CEA will formulate and direct the development of new or revised information security policies and strategies based on these ongoing changes to ensure CalSTRS continued commitment to protecting the confidentiality, integrity and availability of the information assets of CalSTRS and its members.