

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

5/28/2020

2. Department

Office of Legislative Counsel

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

Legislative Data Center/ Legislative Technology Branch

4. CEA Position Title

Chief Information Security Officer

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

The Office of Legislative Counsel (OLC) proposes to create a new CEA Chief Information Security Officer (CISO) position to fulfill the OLC's mission to provide excellent, timely, and nonpartisan legal and legislative technology services to meet client needs. Under the administrative direction of the Chief Deputy Director of the Legislative Technology Branch within the Legislative Data Center (LDC) of the OLC, the CISO will provide leadership, management direction, and policy guidance to the LDC Information Security Program. The CISO plans, organizes and directs activities associated with the following LDC Information Security Program: Security Architecture, Vulnerability Assessment, Risk Assessment, Incident Management, Audit Compliance, Policy Compliance, Threat Detection, Incident Response, Investigation, Security Operations, and Education and Awareness Training. 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 LDC assets. The CISO will have frequent contact with the OLC Executive Management Team and be an expert policy advisor to the Legislative Counsel, with regular contact with high-ranking legislative staff and members of the California Legislature.

6. Reports to: (Class Title/Level)

CEA - Chief Deputy Director/1st Organizational Level

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 CEA CISO position (2nd organizational level) will report to the Chief Deputy Director second organizational level) of the Legislative Technology Branch within the Legislative Data Center of the OLC and will be a key advisor to the Legislative Counsel, with frequent contact with the Executive Management Team and regular contact with high-ranking administrators of the California Legislature.

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 administrative direction of the Chief Deputy Director of the Legislative Technology Branch within the LDC of the OLC, the CEA Chief Information Security Officer (CISO) will provide leadership, management direction and policy guidance to the LDC Information Security Program. The CISO plans, organizes and directs activities associated with the following LDC Information Security Program: Security Architecture, Vulnerability Assessment, Risk Assessment, Incident Management, Audit Compliance, Policy Compliance, Threat Detection, Incident Response, Investigation, Security Operations and Awareness Training. 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 Legislative Data Center assets. The CISO will have frequent contact with the OLC Executive Management Team, will serve as an expert policy advisor to the Legislative Counsel, and have regular contact with high-ranking legislative staff and members of the California Legislature.

The CISO is responsible for administrating a strategic, comprehensive information security program to ensure appropriate levels of confidentiality, integrity, availability, and privacy of information assets under the custody of or processed by the LDC. The CISO plans and executes the LDC information security policy, strategy and best practices. The CISO collaborates with the other LDC divisions to maintain security standards and action plans to implement best practices. The CISO ensures alignment of the information security vision and strategy with organizational priorities to enable and facilitate business objectives of the OLC and the California Legislature. The CISO works effectively with other LDC divisions to facilitate information security risk assessment, risk management and compliance.

The CISO acts as the principal information security policy maker and has authority for making high-level information security policies. The CISO has significant policy influence and involvement with the creation of new information security policies and implementation thereafter.

The CISO is responsible for hiring, developing and retaining competent and professional staff to assure an adequate level of specialized analytical and technical expertise to support current and future LDC needs; responsible for defining performance expectations. Communicates LDC, Division, and team priorities and objectives to staff and facilitates feedback from staff. Ensures OLC policies and procedures are followed. Establishes work assignments, provides management direction and evaluates work quality and customer satisfaction. Creates and maintains a working environment that fosters skills development in staff, identifies and utilizes training opportunities, and provides developmental or corrective training as required. Ensures that an analytical and technical training program is developed, maintained and executed. Monitors progress on assignments and takes appropriate action to ensure timely and successful completion. Motivates staff to achieve and sustain high performance.

The CISO meets with legislators, the Chief Administrative Officer of the Assembly Rules Committee, the Executive Officer of the Senate Rules Committee, the Assembly Chief Clerk, the Secretary of the Senate, the Chief Information Officers of the two houses, chief consultants to legislative committees, and other high-level legislative staff to provide information security briefings, identify business priorities and resolve critical problems. Acts as an advocate for information security best practices for LDC and LDC customers.

The CISO manages information security awareness training for all OLC employees and contractors, and establishes metrics to measure the effectiveness of the security training program.

The CISO maintains information security professional networks consisting of technology vendors and other public organizations and legislatures to address trends, findings, incidents and cybersecurity risks. Acts as a liaison with external agencies such as law enforcement and other advisory bodies as necessary

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 OLC is a small state department excluded from collective bargaining and comprised of legal, information technology and administrative divisions that provide essential and confidential legal and legislative technology services to the California Legislature, and make legislative information available to the public. Without the support of a robust and proactive information security program, the OLC would be unable to provide services upon which complex and politically-sensitive legislative processes are dependent. Further, without the necessary support for the management of new information security policies and services, the legislative process would be significantly impacted.

Information is a valuable asset to be protected from unauthorized access, inspection, use, disclosure or modification. The Legislative Data Center is committed to protecting the confidentiality, integrity and availability of information assets as entrusted by the OLC and Legislature and does so via its dedicated Information Security Program. The CISO will develop, implement and maintain policies, standards, procedures and guidelines for information security management to ensure the security, confidentiality, integrity, availability and privacy of the Legislative Data Center's information assets. The CISO will serve as an expert policy advisor to the Legislative Counsel and OLC executive staff, as well as have regular contact with high-ranking legislative staff and members of the California Legislature. The CISO will oversee activities to monitor and evaluate conditions in the internal and external environment including the ongoing potential risk of cyber-terrorism or computer hacking that would negatively impact information security, financial, operational and/or the reputation of OLC and the Legislature.

Because the legislative process depends upon the reliability, availability and credibility of data and systems, information security is an essential management function. Inadequate information security management would have a significant impact on the legislative process.

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.

There are two factors driving the need to establish a CEA position to serve as the Legislative Data Center's CISO of the Information Security Division: the increase in use of mobile and remote access technologies; and, the need for LDC to secure legislative information as well as maintain the data integrity of legislative information in the face of ongoing and increasing cyber threats and proliferation of consumer Internet of Things (IoT) devices in the legislative work environment.

1. Increase in use of mobile and remote access technologies: The use of various mobile devices was recently implemented in the California State Assembly in support of an application used by members of the Assembly to access via mobile devices the information essential in conducting the legislative process. There has also been a marked increase in providing mobile access to office automation, document sharing and collaboration tools, such as instant messaging and video conferencing and the proliferation of consumer IoT devices on internal and public platforms. In addition, there has been an increase in deployment of mobile-accessible applications such as training systems, supply systems, inventory systems, and several intranet sites delivering content to mobile devices supporting the legislative process.

The accompanying infrastructure requirements for mobile application platforms and mobile device deployments involve complex information security services policies and processes necessary for ensuring information is protected.

2. Increase in cybersecurity and computer hacking threats: Cybersecurity threats are becoming a day-to-day challenge for business. Recent trends and cybersecurity statistics indicate that with the upsurge in social media usage, there is a significant increase in hacked and breached data from mobile and IoT devices. According to 2020 research findings by Symantic Corporation, IoT devices experience an average of 5,200 attacks per month, and 1 in 36 mobile devices had high- risk applications installed. Symantic also cites a 43 percent increase in social media fraud attacks as well as 70 percent increase of fraudulent transactions originating from mobile devices in 2018. Further, as per RSA Security, one of the global leaders on data encryption and encryption standards, fraud from mobile applications has increased 680 percent since 2015. The increase in cybersecurity threats and hacking incidents over the years make it necessary to increase resources developing and maintaining the OLC Information Security Program.

With the prevalence of cybersecurity threats impacting mobile technologies, LDC is responsible for pro-actively addressing security needs in a changing business and technology environment. This responsibility requires keeping pace with an evolving threat landscape to ensure security of information assets. Information security is one of the primary risks to the organization, as the OLC's reputation and customer confidence would be damaged as a consequence of inadvertent, unauthorized, or malicious disclosure of confidential and/or sensitive information, or an information systems breach resulting in disruptions to the legislative process.

Since the delivery of services, supporting the legislative process depends upon the reliability and credibility of data and systems, there is a pressing need to increase the focus on improving critical security infrastructure. The CISO provides oversight to the Information Security Office (ISO) who is responsible for security policies, standards and procedures to protect the confidentiality, integrity, and availability of information assets for the Legislature and OLC. The ISO is critical to ensuring LDC defends against internal and external threats to its data and information assets.

In 2019, to meet business needs for strengthening security operations, LDC moved its Network Engineering section into the Information Security Services section. The ISO has full management responsibility for the LDC Security Operations and Network Engineering Section to ensure the security of the legislative network, hardware, software, data of the enterprise, engineering, architecting, design, implementation, operation, and support of the California Legislative Network. The California Legislative Network is comprised of a wide area network that connects more than 300 legislative district offices throughout the State of California and a local area network that connects the Capitol, Legislative Office Building, legislative support offices and Office of Legislative Counsel at 915 and 925 L Street, and the Legislative Data Center at 1100 J Street. The Security Operations Section is a 24 hour by 7 day, centralized facility with personnel monitoring LDC's information assets, systems, and infrastructure and performing analysis, investigation, reporting and remediation on internal and external threats based upon security incidents, events and hunting campaigns. The Security Operations section actively manages security threats, vulnerabilities, events and incidents to ensure the availability of critical systems and strengthen LDC's overall security. Moving Network Engineering under management by the ISO and under direction of the CISO enables LDC to develop, fortify and implement more robust information security strategies as necessary to protect the confidentiality, integrity and availability of the legislature's information assets and to effectively monitor and respond to cyber threats. This increased level of responsibility and scope along with aforementioned factors requires the establishment of a CEA to serve as CISO 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.

The CISO provides direction and policy guidance to the LDC. The LDC CISO has broad decision-making authority and management responsibility for protecting the confidentiality, integrity, and availability of LDC information and services.

The CEA will be the principal policy maker for the following:

1. Security policies and criteria for protecting and using information assets under the custody of the LDC, including, but not limited to: preventing unauthorized access, corruption, disclosure, or destruction of LDC's information or information systems to ensure the security, availability, and confidentiality of information assets. In protecting LDC's assets, the CISO protects attorney-client confidential data for legal services, privacy of constituent cases, as well as legislative employees' personnel, payroll, and financial data.
2. Policies for the CISO to monitor and ensure LDC's perimeter defense systems are secure from internal and external threats. This includes policies related to activating incident response and communicating active or detected threats and exploits to the Legislative networks and systems. The decisions made in this area will be essential to managing security threats, reducing their impact to the LDC and its customers, and ensuring systems critical to LDC's operations are available to support the ongoing operations of the Legislature.
3. Policies that provide operational guidance in securing network equipment and software, communications and media, and physical security systems related to data transmittal and storage. The policies will ensure that connectivity between the Capitol, District Offices, Legislative Office Building, Legislative Analyst's Office, Office of Legislative Counsel facilities, and business partners is guarded against intrusions.
4. Policies that provide security awareness education and establishing training guidelines for OLC staff. This includes policies that educate employees on awareness, prevention, detection and best practices that help reduce cybersecurity threats and vulnerabilities.
5. Mobile Device Policies that provide acceptable use and definition of standards, procedures, and restrictions for end users who have legitimate business requirements to use mobile devices that can access Legislative applications and information.

The statewide impact of these policies impact over 3,200 internal users including the Office of Legislative Counsel, Legislative Data Center, the California Legislature, Legislative Analyst's Office, other business partners and the public. Statutory requirements mandate that legislative information such as bill text, codes, votes, and recorded hearings be available to the public. Failure in the enactment of these policies inhibits the ability of the Legislature to operate and disrupts the public's ability to be privy to those operations.

C. ROLE IN POLICY INFLUENCE (continued)

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

The OLC has a high degree of accountability to the California Legislature, and is therefore expected to be more diligent with business in comparison to other state departments. The mission-critical support the OLC provides to legislators and their respective staff ensures the California Legislature has a robust and proactive information security program that is committed to the protection of legislative data and the growth of an information security-minded culture with the California State Legislature.

The CISO will have broad decision-making authority in the development, revision, recommendation, and implementation of policies and procedures related to the full scope of the security and monitoring of LDC's information assets. The CISO will be required to identify resolutions to problems by developing timely and effective strategies to improve the Information Security Program in accordance with applicable laws, rules, and regulations, as outlined below:

The CISO is responsible for the implementation and management of the following enterprise-wide programs: The Information Security Program, which consists of policies, standards, and procedures to protect the confidentiality, integrity, and availability of LDC's information assets and to ensure LDC is in compliance with governing authorities; the Risk Management Program, which consists of ongoing system categorizations, data classifications, and risk assessments, and developing mitigation strategies to reduce the probability and impact of risks; the Incident Response Program, which consists of the intake, processing, and reporting of information security incidents, and overseeing departmental incident response communications; and the Information Security Awareness and Training Program, which consists of continuous efforts to provide information security expertise as well as awareness, guidance, and education to LDC information assets users on information and cybersecurity issues.

The CISO is responsible for continuously monitoring LDC's information assets, systems, and infrastructure and performing analysis, correlation, investigation, reporting, and remediation of internal and external threats based on security incidents, events, and hunting campaigns. The CISO core functions include around-the-clock monitoring, cyber threat intelligence analysis, forensic and malware analysis, threat hunting, incident response, and client services support.

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

The CEA will be responsible for developing new policy and revising existing policy. The CEA will serve as a key advisor and resource to the Legislative Counsel, OLC Executive Management and high-ranking legislative staff and members of the California Legislature regarding information security matters. The CEA will manage, administer, and monitor the Information Security Program in response to business needs and industry trends as is necessary to meet operational requirements and to decide upon future program practices.