

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

07/07/2017

2. Department

California Department of Technology

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

Office of Information Security

4. CEA Position Title

Deputy 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 California Department of Technology (CDT) is requesting approval to establish the Deputy Chief Information Security Officer (Deputy CISO) for the Office of Information Security (OIS) at the CEA level. The CEA will oversee operations and will be key in the creation of a State government culture that places a high value on the security of State information, information assets, and the protection of personal information. The CEA will be involved in a broad range of activities within the state and collaborate with federal, state and local security professionals, higher education, private industry, and others on security-related matters.

6. Reports to: (Class Title/Level)

State Chief Information Security Officer, Exempt, 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):

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 Deputy CISO is responsible for the development, maintenance, implementation and enforcement of statewide policies to ensure the CDT can provide for the safety and security of the technical infrastructure and the data and information of California State Organizations. The Deputy CISO will have primary responsibility for managing the Security Operations, which includes Security Assurance, Security Solutions and Security Threat Management, also known as Security Operations Center (SOC). The CEA's responsibilities include implementing physical and information technology (IT) security systems; strategic and operational planning (internal and external); the development and implementation high-level statewide IT policies and procedures addressing detection, prevention, containment and deterrence mechanisms to protect and maintain the integrity of the CDT technical infrastructure and data files for departmental and program security and recovery; and ensuring overall coordination and integration of data center security policies, programs and plans. The CEA must have an extensive understanding of the State's IT enterprise and programs, and emerging technological trends and use this knowledge to communicate to all appropriate audiences. As a member of the Executive Staff, the CEA will participate directly in setting and implementing policies that affect the CDT and its customers. The Deputy CISO will advise the State Chief Information Security Officer (CISO) and the Executive Staff on all policy decisions affecting physical and IT security for the CDT. The Deputy CISO will work in conjunction with executives and management staff from other State departments, industry executives, the Governor's Office, control agencies, and information security professional organizations in establishing statewide policies that affect the security of the CDT and its customers. Specifically, the Deputy CISO's responsibilities would include:

- Implementing and maintaining risk management for the CDT and assisting the CDT customers in implementing and maintaining their risk management programs.
- Reviewing existing operations and engineering policies and processes at the CDT and recommending policy/procedural/process changes, for further efficiencies and effectiveness, to the highest levels of the CDT management.
- Identifying vulnerabilities that may cause inappropriate or accidental access, destruction, or disclosure of confidential information and establish policies and controls necessary to eliminate or minimize their potential effects.
- Implementing and operating a software auditing program to ensure that the CDT policies and procedures are followed.
- Developing and implementing the Computer Security Incident Response Program policies and processes used at the CDT and oversee the execution of Incident Response activities. Developing and implementing the policies and processes that the CDT will use when working with customer agencies without experienced and knowledgeable Incident Response policies and capabilities.
- Establishing cooperative relationships with Office of Technology Services (OTech) management within CDT to keep them abreast of related incidents and/or security events and investigations resulting from SOC and/or security operations branch analysis.

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 mission of the CDT is to be committed to partnering with state, local government and educational entities to deliver digital services, develop innovative and responsive solutions for business needs, and provide quality assurance for state government IT projects and services.

The OIS is an office within the CDT. The CISO is the primary state government authority charged with ensuring the confidentiality, integrity, and availability of state systems and applications, and ensuring the protection of state information assets. The CISO is involved in a broad range of activities within the state and collaborates with federal, state and local security professionals, higher education, private industry, and others on security related matters. The CISO is committed to securing the state's information assets to build and maintain the trust of Californians.

The OIS is statutorily mandated by law to safeguard the confidentiality, integrity and availability of state information, systems, and applications, to promote and protect the development of IT infrastructure and networks, and ensure the uninterrupted operation of mission critical state programs. In order to properly execute this undertaking, OIS has directed its existing resources within four core objective areas: (1) Security Management (Security Assurance, Solutions and Operations), (2) Oversight (Audits and Assessments), (3) Security Risk Governance and (4) Advisory Services. These four areas are integrated and interdependent in their mission, common goals and objectives to ensure the protection of the State's information security assets and data. Today's cybersecurity landscape changes rapidly and the number and type of threats evolve faster than the technology, processes, policies and oversight currently in place to adequately protect against them. Without this investment, OIS lacks the necessary resources to identify, protect, detect, respond and recover from cybersecurity incidents. Each of the problems and solutions described are interdependent and a vital part of the State's cybersecurity defense.

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 primary reason for a Deputy CISO is the result of the dramatic up-tick in responsibility and the need for developing and updating statewide policies surrounding the increased duties of the CISO, which now incorporates all of internal CDT security and external (customer) facing security solutions and products to include various security solutions (in the Security Solutions branch), such as vulnerability management and architecture review. The CEA leadership representative in these incidents would be required to be on-call for CDT and OTech (statewide data center) incidents, as well as work directly with the California Department of the Military, the California Highway Patrol (CHP) and California Cybersecurity Integration Center (CAL CSIC) in the event of a large scale cybersecurity emergency. The latter example would require an executive-level position be available to respond 24 hours a day, 7 days a week, in order to help guide the response of the state in the moment of a crisis should the need arise.

Additionally, the traditional role of OIS has morphed from the initial office mission from setting statewide cybersecurity policy, standards, and procedures to now include conducting audits and independent security assessments, training and/or providing customer facing resources (such as advisory services) for ISO and AISOs to help improve their information security program. To ensure that these new functions, including the aforementioned security operations function, are adequately conducted, a Deputy CISO is needed to load share the vast amount of new mission critical work. The Deputy CISO would also be responsible as stepping in as the State CISO in case of absence.

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 Deputy CISO will develop and implement high-level policy, both Statewide and department- wide, to ensure the procedures and tools that can provide for the integrity and security of the IT infrastructure and information for State organizations are in place. These high-level policies cover risk management, asset protection, vulnerability management, threat management, appropriate use and security awareness and education for the CDT and customer assets and systems managed by the CDT.

Statewide IT Policy – Pursuant to Government Code Sections 11541-11546 and 11549.3, the California Department of Technology (CDT) exercises independent responsibility for establishing, maintaining, and enforcing statewide policies related to IT operations, IT services, security, project approval, telecommunication systems, procurement, enterprise architecture, accessibility, and oversight while ensuring alignment with the State's IT strategic goals. The CDT Statewide IT Policy Office is tasked with carrying out these functions while planning and managing statewide standards, instructions, and guidelines.

As set forth in Government Code section 11549.3, state entities shall comply with the information security and privacy policies, standards and procedures issued by the California Information Security Office (CISO). In addition to compliance with the information security and privacy policies, standards, procedures, and filing requirements issued by the CISO, state entities shall ensure compliance with all security and privacy laws, regulations, rules, and standards specific to and governing the administration of their programs. Program administrators shall work with their general counsel, Information Security Officer (ISO), and Privacy Program Officer/Coordinator to identify all security and privacy requirements applicable to their programs and ensure implementation of the requisite controls.

The policies established by CDT cover risk management, asset protection, vulnerability management, threat management, appropriate use and security awareness and education for the CDT and customer assets and systems managed by the CDT. The CDT policies must work in close concert with risk management and information security policies and processes in place in customer agencies, and, in many cases, determine the information security policies and processes that can be used by customers. Specifics include:

- Establishing policies and governance management for CDT and OTech surrounding the statewide wide area network (CGEN). These policy areas have impact to all CGEN customers (over 100), as well as any data center and tenant managed customer residing in the OTech data center.
- Establishing and monitoring policies related standards and the operational processes that provide for the integrity and security of automated information produced or used in the course of department and customer agency operations in compliance with State and federal mandates.
- Establishing policies which provide for the security of the CDT IT facilities throughout the State.
- Establishing policies and standards defining software and equipment that the CDT uses to protect automated information processing systems and data used by customers.
- Establishing policies for and ensuring that the department has implemented the network hardware and software elements to provide the necessary information security infrastructure used by all customer systems and programs. This includes ensuring the installation and maintenance of security software and hardware for vulnerability management and threat management processes on all the CDT computer systems and networks.
- Establishing and maintaining policies for an IT risk management program, including a risk analysis program.

Governing Provisions: Government Code section 11549.3 provides the CISO with the responsibility and authority to create, issue, and maintain policies, standards, and procedures; direct each state entity to effectively manage risk; advise and consult with each state entity on security issues; and ensure each state entity is in compliance with the requirements specified in the State Administrative Manual (SAM) Chapter 5300.

Government Code section 11549.3 also provides the CISO with the responsibility to coordinate the activities of state entity ISOs for purposes of integrating statewide security initiatives and ensuring compliance with information security and privacy policies and standards. The CISO is also provided with the authority to conduct, or require to be conducted, independent security assessments or audits of any entity. The cost of such assessments or audits shall be funded by the state entity being assessed or audited.

Additionally, as outlined in Technology Letter 16-05 issued May 2016, the CDT CISO issues policy and procedures to further assist Agencies/ state entities to comply with information security and privacy requirements. As the use of computers and automated systems has increased, so has the need for stronger security and controls to manage and protect private information. In an effort to improve incident reporting, the CISO has replaced manual and redundant incident reporting processes with an automated security compliance and reporting system. This improvement was needed to maximize effectiveness so resources can continue to meet statutory mandates.

The new California Compliance and Security Incident Reporting System (Cal-CSIRS) will fully integrate the statewide information security program compliance functions, improve and streamline compliance reporting processes and provide greater situational awareness through management reports and dashboards. Cal-CSIRS will be implemented in multiple phases; the incident reporting module and corresponding procedures are being implemented in this first phase.

C. ROLE IN POLICY INFLUENCE (continued)

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

The scope of the Deputy CISO is broad and extensive. The decisions made have a statewide enterprise impact to multiple departments with responsibility and authority to create, issue, and maintain policies, standards, and procedures. The CEA has authority to direct each state entity to effectively manage risk; advise and consult with each state entity on security issues; and ensure each state entity is in compliance with the requirements specified in the State Administrative Manual (SAM) Chapter 5300.

The Deputy CISO will be responsible for establishing and maintaining policies and processes that protect the IT assets managed by the CDT, which are worth hundreds of millions of dollars. The scope covers the CDT business offices and training facilities, the CDT data centers, including the power supplies and generators for emergency operations, the mainframe computers used to support State customers, the server-based systems and storage systems used by CDT and its customers, the network infrastructure that delivers information to and from and between customers, the specialized computer programs used by State government, and the multi-terabyte data bases and data files of public and confidential information from customers to protect against unauthorized or accidental access, use, duplication, modification or destruction.

The Deputy CISO will exercise broad independence of action under legislative and control agency policies and oversight. Contacts include federal agencies, State control agency staff, the Governor's Office, Government Operations Agency, Chief Information Officers (CIOs), Chief Information Security Offices, and Data Processing Manager IIIs through CEA Cs. The CEA will work collaboratively with the CHP, the California Department of the Military, Office of Health Information Integrity, and other essential agencies on mitigating, identifying, responding to, and reporting information security incidents.

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

The evolution of technology will continually require the CEA to develop new statewide IT policies that will impact all state departments that rely on technology to support their critical business programs. The CEA will be responsible for initiating and implementing new policies and revising existing policies necessary to enforce statewide policies related to IT operations, IT services, IT Security, project approval, telecommunication systems, procurement, enterprise architecture, accessibility, and oversight while ensuring alignment with the State's IT strategic goals.

As technology progresses to meet the evolving needs of the public, IT policies and authorities must also evolve to remain relevant and current. The California governance model for technology helps to determine the state's IT policy and portfolio, reduce bureaucracy, and focus on tangible results.