California
DEPARTMENT OF TECHNOLOGY

STATE OF CALIFORNIA
Governor
Gavin Newsom

CAREER EXECUTIVE ASSIGNMENT EXAMINATION ANNOUNCEMENT

DEPARTMENT: California Department of Technology

POSITION TITLE/LEVEL: Deputy State Chief Information Security Officer, CEA C
Office of Information Security

SALARY: $ 11,505 - $ 13,063

FINAL FILE DATE: **April 22, 2021**

POSITION DESCRIPTION:
Under the general direction of the State Chief Information Security Officer (State CISO), the Deputy State Chief Information Security Officer (Deputy State CISO) is responsible for the development, maintenance, implementation and enforcement of statewide policies to ensure the California Department of Technology (CDT) can provide for the safety and security of the technical infrastructure and the data and information of California State Organizations. The Deputy State CISO will have primary responsibility for managing the Risk Governance, Advisory, Audit/Compliance, and Security Operations, which includes Security Assurance, Security Solutions and Security Threat Management, also known as Security Operations Center (SOC). The Deputy State CISO will be focused on execution and promotion of statewide security strategy. The Deputy State CISO will also have responsibility over the operational support of Incident Response and threat intelligence staff embedded within the California Cybersecurity Integration Center (Cal-CSIC) within the Governor's Office of Emergency Services.

The Deputy State CISO's responsibilities are:

- Develop, implement and enforce statewide Information Technology (IT) security policies to ensure the safety and security of the technical infrastructure for the State.
- Implement physical and security systems; strategic and operational planning (internal and external); develop and implement 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 ensure overall coordination and integration of data center security policies, programs and plans.
- Implement and maintain risk management for the CDT and assist the CDT customers in implementing and maintaining their risk management programs.
- Review existing operations and engineering policies and processes at the CDT and recommend policy/procedural/process changes for further efficiencies and effectiveness to the highest levels of the CDT management. Identify 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. Implement and operate a software auditing program to ensure that the CDT policies and procedures are followed.
- Define the Computer Security Incident Response Program policies and processes used at the CDT and oversee the execution of Incident Response activities.

- Participate in establishing Risk Governance processes within departments to provide security risks, mitigations, and input on other technical risks. Participate as the statewide risk advisor to entities and all statewide project initiatives on risk management.
- Serve as a member of the department's Executive Staff; act as an advisor to the Director/State Chief Information Officer (CIO), Chief Deputy Director/Deputy State CIO, and the CISO on security-related governance, risks and remediation.
- Must pass a fingerprint background check completed by the Department of Justice (DOJ) and Federal Bureau of Investigation (FBI) as a condition of employment.

MINIMUM QUALIFICATIONS
CEA examinations are open to all applicants who possess the knowledge and abilities, and any other requirements as described in the examination bulletin. Eligibility to take a CEA examination does not require current permanent status in civil service. Applicants must possess the ability to perform high administrative and policy-influencing functions effectively. Such overall ability is demonstrated by the following more specific knowledge and ability requirements:

A. REQUIRED KNOWLEDGE:

1. Knowledge of the organization and functions of California State Government, including the organization and practices of the Legislature and the Executive Branch;
2. Knowledge of the principles, practices, and trends of public administration, organization, and management;
3. Knowledge of the techniques of organizing and motivating groups;
4. Knowledge of program development and evaluation;
5. Knowledge of facilitation and negotiation techniques to promote collaboration amongst diverse groups;
6. Knowledge of the methods of administrative problem solving;
7. Knowledge of the principles and practices of policy formulation and development; and personnel management techniques;
8. Knowledge of the department's Equal Employment Opportunity Program objectives; and a manager's role in the Equal Employment Opportunity Program.
9. Knowledge of cybersecurity operations and incident response practices and experience leading security analysts and technical staff in finding and remediating security threats.
10. Knowledge of cybersecurity policies and industry best practices such as the National Institute of Standards and Technology (NIST) special publications and the Center for Information Security Top 20 Security Controls.
11. Extensive experience in security management, legislation and policy making.
12. Experience as an Information Security Officer for a state government department, state government agency, or large multi-national private sector corporation.
13. Industry cybersecurity certifications, such as Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Global Information Assurance Certification (GIAC) Security Leadership Certification (GSLC), or other information security accreditations.

B. REQUIRED ABILITIES:

1. Ability to plan, organize, and direct the work of multidisciplinary professional and administrative staff;
2. Ability to analyze administrative policies, organization, procedures, and practices;
3. Ability to integrate the activities of a diverse program to attain common goals;
4. Ability to gain the confidence and support of top level administrators and advise them on a wide range of administrative matters;
5. Ability to develop cooperative working relationships with representatives of all levels of government, the public, and the Legislature and Executive branches;
6. Ability to analyze complex problems and recommend effective courses of action; and prepare and review reports;
7. Ability to effectively contribute to the department's Equal Employment Opportunity objectives.
8. Ability to work with a wide range of senior level executives and state employees on time sensitive and confidential incidents and reports.

SPECIAL PERSONAL CHARACTERISTICS

- Creativity and Innovation – Apply new ways of thinking, ability to solve problems, create new ideas, and develop new approaches to optimize the organization and management of IT programs. Survey the landscape and recommend/develop new services that help customers meet their business needs.
- Teamwork – Cooperate to achieve the California Department of Technology's mission, goals and values, and encourage a diversity of opinions. Ability to facilitate cross-agency collaboration activities. Ability to build and manage high-level teams.
- Continuous Improvement – Focuses on continuous improvement and high personal accountability. Provides leadership that assures his/her management team and staff maintains this focus as well.
- Communication – Ability to interact and communicate effectively with executive management at the State level, as well as various private and public organizations. Ability to interact in a diplomatic, tactful and effective manner with all levels of staff. Ability to negotiate win-win solutions in difficult and challenging situations. Ability to speak and write clearly, and effectively.

DESIRABLE QUALIFICATIONS

In addition to the above, the following experience factors will be considered in competitively evaluating each candidate:

- Industry cybersecurity certifications, such as Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), and Global Information Assurance Certification (GIAC) Security Leadership Certification (GSLC).
- Extensive experience in security management, legislation and policy-making.
- Knowledge of organization and functions of California State government, including the organization and practices of Control Agencies, Legislature and the Executive Branch.
- Ability to communicate effectively with others as demonstrated by strong written and verbal communication skills, strong negotiating skills, and particularly the ability to represent the California Department of Technology effectively with the Administration, control agencies, Legislature, key customers, stakeholders and internal staff.
- Experience in obtaining buy-in and providing leadership to a large group of multi-disciplinary team members that do not report directly to the incumbent.
- Knowledge of the structure, organization and function of a variety of technology disciplines, as well as local, State and federal initiatives and programs.
- Ability to anticipate and manage complex information security issues affecting many organizations, including the ability to develop policy and integrate all aspects of a strategy to assure resolution of issues.

- Proven track record of gaining the confidence and trust of individuals in key positions in the department's customer base.
- Ability to evaluate products from multiple perspectives (customers, stakeholders, vendors, best practices) in order to develop standards for product approvals.
- Ability to develop/obtain consensus on policy direction that will ensure the State's safeguards again cybersecurity attacks, and the secure operation of the State's IT infrastructure.

EXAMINATION INFORMATION – STATEMENT OF QUALIFICATIONS

This examination will consist of a review of the candidates' application and Statement of Qualifications by an executive screening committee, using predetermined evaluation criteria. Candidates will be screened on the basis of their background and demonstrated management experience as detailed in the Statement of Qualifications. The Statement of Qualifications may be the only basis for determining your final score and rank on the eligible list.

Interviews may be conducted as part of the examination process. (Hiring interviews may be conducted with only the most qualified candidates if it is determined necessary in order to make a selection.) All applicants will be notified of their examination results. In order to be successful in this examination a minimum rating of 70 percent must be attained. The results of this examination may be used to fill subsequent vacancies in this position if they occur within the next twelve months, or an examination may be rescheduled, at the discretion of the department.

FILING INSTRUCTIONS

- A Standard original State application (Form 678) is required.
- Prepare a "Statement of Qualifications" **not to exceed three pages**. This "Statement of Qualifications" is a narrative discussion of the candidate's education and experience that would qualify them for the Deputy State Chief Information Security Officer (Deputy State CISO) position.

Each candidate's Statement of Qualifications **must clearly and concisely identify experience in the following 4 categories and be formatted in the same manner as shown below**

1. **Policy Experience**
   Describe the type of Policy Experience you possess and how that experience will further the objectives and goals of the Office of Information Security.
2. **Strategic Planning Experience**
   Describe the type of Strategic Planning initiatives you have developed or implemented and your primary role and responsibility at that time. This experience does not have to be cybersecurity related and can include things such as organizational or operational planning and implementation experience.
3. **Organizational Change Management**
   Describe your experience addressing Organizational Change and what techniques you used.
4. **Information Security Expertise**
   Describe the Information Security Expertise you possess that demonstrates you are the most qualified candidate to serve as the California Department of Technology Deputy State CISO. In addition, please identify two key accomplishments within the last 12 months.

Candidates who do not follow the filing instructions will be disqualified from the examination.

(**Note:** A résumé does not serve as a Statement of Qualifications.)

The application and "Statement of Qualifications" are to be submitted via online at www.calhr.ca.gov JC#242111 or by mail (postmarked no later than April 22, 2021) to:

California Department of Technology
Human Resources Branch
P.O. Box 1810
Rancho Cordova, CA 95741-1810
Attn: Rae Powers JC#242111

or
Hand Delivered (no later than 5:00 p.m. on April 22, 2021) to:
California Department of Technology
2nd Floor Guard Station
10860 Gold Center Drive
Rancho Cordova, CA 95670
Attn: Rae Powers JC#242111

Questions regarding this examination should be directed to: Rae Powers at (916) 431-4059 or e-mail Rae.Powers@state.ca.gov

TDD is Telecommunications Device for the Deaf and is reachable only from phones equipped with a TDD Device.
California Relay (telephone) Service for the Deaf or Hearing impaired From TDD phones: 1-800-735-2929
From voice phones: 1-800-735-2922

DUTY STATEMENT
DEPARTMENT OF TECHNOLOGY
DEPUTY STATE CHIEF INFORMATION SECURITY OFFICER
OFFICE OF INFORMATION SECURITY

Name:
Effective Date: xx/xx/2021

SCOPE:

Under the general direction of the State Chief Information Security Officer (State CISO), the Deputy State Chief Information Security Officer (Deputy State CISO) is responsible for the development, maintenance, implementation and enforcement of statewide policies to ensure the California Department of Technology (CDT) can provide for the safety and security of the technical infrastructure and the data and information of California State Organizations. The Deputy State CISO will have primary responsibility for managing the Risk Governance, Advisory, Audit/Compliance, and Security Operations, which includes Security Assurance, Security Solutions and Security Threat Management, also known as Security Operations Center (SOC). The Deputy State CISO will be focused on execution and promotion of statewide security strategy. The Deputy State CISO will also have responsibility over the operational support of Incident Response and threat intelligence staff embedded within the California Cybersecurity Integration Center (Cal-CSIC) within the Governor's Office of Emergency Services.

SPECIFIC DUTIES:

30% Develop, implement and enforce statewide Information Technology (IT) security policies to ensure the safety and security of the technical infrastructure for the State. Implement physical and security systems; strategic and operational planning (internal and external); develop and implement 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 ensure overall coordination and integration of data center security policies, programs and plans. Participate within the Cal-CSIC broader cybersecurity role within local, county, municipal, academic and special district jurisdictions. Participate directly in setting and implementing policies that affect the CDT and its customers, and providing support for State and local cybersecurity incident response engagements.

30% Implement and maintain risk management for the CDT and assist the CDT customers in implementing and maintaining their risk management programs. Review existing operations and engineering policies and processes at the CDT and recommend policy/procedural/process changes for further efficiencies and effectiveness to the highest levels of the CDT management. Identify 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. Implement and operate a software auditing program to ensure that the CDT policies and procedures are followed. Track and report program audit findings and recommendations to ensure that appropriate mitigation actions are taken and providing assistance where necessary. Define the Computer Security Incident Response Program policies and processes used at the CDT and oversee the execution of Incident Response activities. Participate in establishing Risk Governance processes within departments to provide security risks, mitigations, and input on other technical risks. Participate as the statewide risk advisor to entities and all statewide project initiatives on risk management.

30% Serve as a member of the department's Executive Staff; act as an advisor to the Director/State Chief Information Officer (CIO), Chief Deputy Director/Deputy State CIO, and the State CISO on security-related governance, risks and remediation. The Deputy State CISO will advise the State CISO and the Executive Staff on all policy decisions affecting physical and IT security for the CDT. Advise the State CISO and the Executive Staff on all policy decisions affecting physical and IT security for the CDT and expand support for Cal-CSIC efforts in cyber threat intelligence. The Deputy State CISO will work in conjunction with executives and Information Security Officers 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. The Deputy State CISO will serve as a member of the Cal-CSIC, State Executive Staff. Provide input to new legislation proposed to strengthened cybersecurity, privacy, emerging security issues, and information security strategies for the future. Develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance, governance/policy, and incident response needs of privacy and security executives and their teams. Develops policies and plans and/or advocates for changes in policy that support organizational cyberspace initiatives or required changes/enhancements. Executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.

10% Provide executive oversight of personnel management and administrative responsibilities; evaluate direct reports on completion of their administrative responsibilities; develop and update duty statements as needed, establish performance expectations, complete individual development plans annually, complete probationary reports on a timely basis, and other performance management activities including adherence to the State's progressive discipline policy including taking corrective or disciplinary action as necessary; ensure management makes informed and defensible personnel management decisions in accordance with department and State policies, personnel-related laws, civil service rules, and collective bargaining agreements; effectively contribute to the department's equal employment opportunity objectives. Ensure that there is a diverse workforce throughout the Office; manage the Office's budget preparation and expenditure control including position management activities and management of vacancies; ensure that managers are doing their part to facilitate communication throughout the division; ensure that appropriate measures are taken when issues and problems arise in the administrative arena; and responsible for succession planning within the Office and ensure there are employees who can perform multiple functions.

DESIRABLE QUALIFICATIONS:

- Industry cybersecurity certifications, such as Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Global Information Assurance Certification (GIAC) Security Leadership Certification (GSLC), or other information security accreditations
- Extensive experience in security management, legislation and policy-making.
- Knowledge of organization and functions of California State government, including the organization and practices of Control Agencies, Legislature and the Executive Branch.
- Ability to communicate effectively with others as demonstrated by strong written and verbal communication skills, strong negotiating skills, and particularly the ability to represent the California Department of Technology effectively with the Administration, control agencies, Legislature, key customers, stakeholders and internal staff.
- Experience in obtaining buy-in and providing leadership to a large group of multi-disciplinary team members that do not report directly to the incumbent.

- Knowledge of the structure, organization and function of a variety of technology disciplines, as well as local, State and federal initiatives and programs.
- Ability to anticipate and manage complex information security issues affecting many organizations, including the ability to develop policy and integrate all aspects of a strategy to assure resolution of issues.
- Proven track record of gaining the confidence and trust of individuals in key positions in the department's customer base.
- Ability to evaluate products from multiple perspectives (customers, stakeholders, vendors, best practices) in order to develop standards for product approvals.
- Ability to develop/obtain consensus on policy direction that will ensure the State's safeguards again cybersecurity attacks, and the secure operation of the State's IT infrastructure.

I have read and understand the duties listed above and I can perform these duties with or without reasonable accommodation. (If you believe reasonable accommodation is necessary, discuss your concerns with the hiring supervisor. If unsure of a need for reasonable accommodation, inform the hiring supervisor, who will discuss your concerns with the assigned HR analyst.)

_____ _____

Deputy State Chief Information Security Officer Date

I have discussed the duties of this position with and have provided a copy of this duty statement to the employee named above.

_____ _____

State Chief Information Security Officer Date

H/R Analyst _____