DUTY STATEMENT
DEPARTMENT OF TECHNOLOGY
CAREER EXECUTIVE ASSIGNMENT, LEVEL C
DEPUTY STATE CHIEF INFORMATION SECURITY OFFICER
OFFICE OF INFORMATION SECURITY

Name:
Effective Date:

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 and programs 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 information assets 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. Evolve the Cal-Secure cyber security roadmap and drive adoption within the community.

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. Drive secure adoption of emerging technologies such as safe and secure implementation of Artificial Intelligence (AI). Participate and enhance the implementation and governance around AI. Provide input to new legislation proposed to strengthen cybersecurity, privacy, emerging security issues, and information security strategies for the future. Provide testimony in legislative briefings. Evangelize, educate and raise awareness cyber security awareness with key stakeholder groups at public speaking events. 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 and/or leadership accreditations such as completion of the California IT Leadership Academy program.
- Demonstrated experience leading or coordinating multi-agency cybersecurity collaboration, such as managing joint incident response efforts (e.g., major ransomware events), establishing memorandums of understanding (MOUs), or developing joint threat sharing protocols across departments, state agencies, and/or local/federal partners.

- Proven leadership in managing or modernizing a 24/7 Security Operations Center (SOC), including implementing threat intelligence platforms, managing escalated incident response processes, and integrating playbooks for high-severity events.
- Demonstrated leadership in developing cybersecurity talent pipelines, including mentorship programs, apprenticeship pathways, succession plans, or internal skill-building initiatives for security staff across departments.
- Experience supporting or leading statewide emergency coordination efforts related to cyberattacks, including coordination with the California Office of Emergency Services, National Guard, local jurisdictions, or federal entities such as CISA or FBI.
- Familiarity with integrating cybersecurity efforts across physical, operational, and information security domains within critical infrastructure or essential government services.
- Experience establishing and reporting on performance metrics for cybersecurity maturity, including KPIs for SOC efficiency, risk reduction outcomes, vulnerability management closure rates, or policy adoption across departments.
- History of serving as a trusted advisor to senior leadership across multiple departments or in a federated environment, providing actionable guidance on security posture improvement, strategic investment, or emerging threat response.
- 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.
- Experience within a Law Enforcement Agency and/or participating with law enforcement on cyber investigative matters (to include California Fusion Centers).
- Experience contributing to cybersecurity efforts from multiple organizational perspectives, including:
    - as a departmental or agency Information Security Officer or security leader responsible for implementing cybersecurity operations,
    - as a contributor or leader within a central security service bureau (e.g., CDT OIS or Security Operations Center), and
    - as a participant in a multi-agency coordination or enforcement entity (e.g., Cal-CSIC, High-Tech Crimes Task Force).

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.)

_____ _____

Date

Deputy State Chief Information Security Officer

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

_____ _____

Date

State Chief Information Security Officer

H/R Analyst _____