STATE OF CALIFORNIA
Rev. 05/23

Governor's Office of Planning and Research

# DUTY STATEMENT

| | |
|---|---|
| PROGRAM<br>STATE PLANNING AND POLICY DEVELOPMENT | POSITION NUMBER (Agency – Unit – Class – Serial)<br>368-695-1406-XXX |
| BRANCH<br>Planning and Research | CLASSIFICATION TITLE<br>Information Technology Manager II |
| SECTION/UNIT (If applicable)<br>Administration – Information Technology | WORKING TITLE<br>Chief Information Security Officer |

| | COI | WWG | CBID | TENURE | TIME BASE |
|---|---|---|---|---|---|
| REGIONAL HUB<br>Sacramento | Yes | E | M01 | P | FT |

| | | |
|---|---|---|
| WORK SCHEDULE<br>M-F 8am-5pm | SUPERVISION EXERCISED<br>None | SPECIFIC LOCATION ASSIGNED TO<br>1400 10th Street, Sacramento, CA 95814 |
| INCUMBENT (If known) | | EFFECTIVE DATE |
| PRIMARY DOMAIN (IT positions only) | Information Security Engineering | |

## AGENCY OVERVIEW

The Office of Planning and Research (OPR) serves the Governor and his Cabinet as staff for long-range planning and research and constitutes the comprehensive state planning agency. OPR assists the Governor and the Administration in planning, research, policy development, and legislative analysis. OPR formulates long-range state goals and policies to address land use, climate change, population growth and distribution, urban expansion, infrastructure development, groundwater sustainability and drought response, and resource protection. OPR's budget programs include State Planning and Policy Development, Strategic Growth Council, California Volunteers, Office of Community Partnership and Strategic Communication, Racial Equity Commission, and Youth Empowerment Commission. OPR is a fast-paced, creative work environment that requires staff to have strong collaboration skills, an ability to quickly respond to changing policy needs, and a positive attitude and sense of humor. Proven commitment to creating a work environment that celebrates diverse backgrounds, cultures, and personal experiences.

## GENERAL STATEMENT

Under administrative direction of the Chief Information Officer (CIO), the Chief Information Security Officer (CISO) is responsible for formulating or administering organizational information technology security and privacy policies and programs, specific to the initiation, design, development, testing, operation, and defense of OPR information technology assets and environments, addressing various sources of disruption. The scope of responsibility includes all OPR offices and client agencies and has overall responsibility for OPR's security governance and compliance of its information technology (IT) that supports OPR's critical lines of business, security, privacy requirements and regulations. As a member of executive management, the CISO provides security leadership experience to manage OPR's cybersecurity and risk management programs to meet confidentiality, integrity, and availability of its assets.

| % of time performing duties | Indicate the duties and responsibilities assigned to the position and the percentage of time spent on each. Group related tasks under the same percentage with the highest percentage first. *(Use addition sheet if necessary)* |
|---|---|
| | **ESSENTIAL FUNCTIONS** |
| **35%** | Oversees the governance of security, risk, and privacy requirements for OPR, including but not limited to: security control assessment and planning across OPR's enterprise architecture, websites, networks, systems, offices, and datacenters. Directs the risk management program through planning, developing, coordinating, and implementing security incident response, disaster recovery, and business continuity planning. Responsible for the oversight of the organization's risk appetite and risk tolerance in support of the Office's Strategic Plan by ensuring alignment with business strategies, |

| | |
|---|---|
| | implementation of effective risk assessments and risk response. Collaborates and builds effective partnerships with statewide technology leaders and control agencies and offices. Provides leadership for the development and continuous improvement of, processes and technology to support OPR Cybersecurity risk management activities. Leads establishing and maintaining cybersecurity risk measurement, reporting and management consistently within OPR. Represents the OPR Cybersecurity Risk Management agency-wide in internal and external meetings. Prepares and delivers executive summary presentations for internal and external audiences and performs data analytics and data visualization activities with a strong background and grounding in all aspects of Information Technology as well as Operational Technology. |
| **30%** | Directs the deployment of security infrastructure to ensure security capabilities meet information security requirements and to cover OPR’s threat universe. Performs and reviews technical risk assessments on applications and systems, including data center physical security and environment. Oversees the development of system security plans. Responsible for the direction of the ongoing development and implementation of information and cybersecurity policies, standards, guidelines, and procedures to ensure information security capabilities cover current threat capabilities. Performs internal audits of the information security program to measure conformity with requirements, to seek continual improvement, and to prepare for state audit examinations. Provides oversight, development, and maintenance of OPR’s security business continuity plans, business impact assessment, POAM and supported risk register and asset inventories. Monitors and ensures vendor and contractor supported functions meet OPR security requirements. Provides security compliance direction and consultation to the Office's executive management team, IT management team, contractors, and program staff on all facets of IT policy, planning, management, and operations. |
| **20%** | Promotes, develops, and manages information security and risk management awareness and training programs across the organization. Provides oversight of the organization’s cybersecurity workforce training and awareness process to educate staff on all threats and vulnerabilities and data classification usage. Developing and maintaining an Information Security program that addresses best practices, emerging threats, and compliance with applicable laws and regulations. Partners with IT on technical projects and provides information security oversight. Reviews system architecture and provides guidance, identifies deficiencies, and makes recommendations to facilitate security by design and adherence to policies, procedures, and government standards. Develops baseline security configuration standards for organizational systems and business applications; reviews configurations to ensure systems are consistently deployed based on the required standards. Handles day-to-day implementation, monitoring, and operation of security related hardware, software, applications, managed solutions, and service provider relationships. Leads technical security projects and regularly participates in project and change management meetings. Stays current with new threats; attacker tactics, techniques, and procedures (TTPs)and mitigations. Researches and recommends new security solutions to address emerging threats and to reduce the attack surface. Represents the Information Security Office in a courteous and professional manner; partners and collaborates with IT and other business divisions on technology and risk decisions. Provides excellent internal customer service by monitoring and responding to security service tickets and email. |
| **10%** | Oversees safeguard evaluation cost benefit analysis, budget preparation, key performance indicators, and key risk indicators to provide security metric reports to OPR executive leadership. Responsible for planning, organizing, and maintaining OPR’s security steering committee to meet OPR executive leadership’s risk appetite and risk tolerance. Provides management guidance to staff within the Security Engineering team, ensuring team responsibilities are successfully performed. Maintains a high-performing team through effective recruiting, training, coaching, and mentoring. Measures staff performance with timely delivered performance reviews. Meets regularly with direct reports to discuss individual developmental needs and career aspirations. Assigns work and communicates priorities, monitors progress, seeks priority adjustments, redistributes workload and/or |

secures extensions as needed to meet established deadlines. Provides regular reports to leadership on status of assignments both verbally and in writing. Prepares and participates in the on-call rotation.

## MARGINAL FUNCTIONS

**5%**

Serves as the liaison between OPR, control agencies, and other governmental agencies to initiate various tasks related to information technology management and development. Reviews proposals and correspondence. Identifies and develops key information regarding IT issues and ensures it is current and accessible for decision-making for management. Provides feedback to staff and advises management on the impact. Participates in staff meetings, attend training, provide work status reports, serve on inter-agency working groups, and perform other duties as assigned. Performs other job-related duties as required.

## KNOWLEDGE AND ABILITIES

*Knowledge of:* A manager's responsibility for promoting equal opportunity in hiring and employee development and promotion and maintaining a work environment which is free of discrimination and harassment; the department's Equal Employment Opportunity objectives; and a manager's role in Equal Employment Opportunity and the processes available to meet equal employment objectives.

*Ability to:* Manage through subordinate supervisors; effectively promote equal opportunity in employment and maintain a work environment that is free of discrimination and harassment; and effectively contribute to the department's Equal Employment Opportunity objectives.

**DESIRABLE QUALIFICATIONS:** Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.

**SPECIAL PHYSICAL CHARACTERISTICS:** Persons appointed to this position must be reasonably expected to exert up to 10 lbs. of force occasionally and/or a negligible amount of force frequently or constantly to lift, carry, push, pull or otherwise move objects. Involves sitting most of the time but may involve walking or standing for brief periods of time.

**The statements contained in this duty statement reflect general details as necessary to describe the principal functions of this job. It should not be considered an all-inclusive listing of work requirements. Individuals may perform other duties as assigned, including work in other functional areas to cover absence of relief, to equalize peak work periods or otherwise balance the workload.**

SUPERVISOR’S STATEMENT: ***I HAVE DISCUSSED THE DUTIES OF THE POSITION WITH THE EMPLOYEE AND HAVE PROVIDED A COPY OF THE DUTY STATEMENT TO THE EMPLOYEE.***

| | | |
|---|---|---|
| SUPERVISOR’S NAME (Print) | SUPERVISOR’S SIGNATURE | DATE |

EMPLOYEE’S STATEMENT: ***I HAVE READ AND UNDERSTAND THE DUTIES LISTED ABOVE AND CAN PERFORM THESE DUTIES WITH OR WITHOUT REASONABLE ACCOMMODATION. (IF YOU BELIEVE REASONABLE ACCOMMODATION IS NECESSARY, DISCUSS YOUR CONCERNS WITH YOUR HIRING SUPERVISOR. IF UNSURE OF A NEED FOR REASONABLE ACCOMMODATION, INFORM YOUR HIRING SUPERVISOR, WHO WILL DISCUSS YOUR CONCERNS WITH HUMAN RESOURCES OFFICE).***

| | | |
|---|---|---|
| EMPLOYEE’S NAME (Print) | EMPLOYEE’S SIGNATURE | DATE |

HRO Approved: 07/19/23 BS