STATE OF CALIFORNIA

DUTY STATEMENT

CALIFORNIA PUBLIC UTILITIES COMMISSION

DIVISION Information Technology Services Division	EFFECTIVE DATE: 08/2022
BRANCH/SECTION Information Security Office	CLASS TITLE Information Technology Manager II
WORKING DAYS AND WORKING HOURS Monday through Friday 8:00 a.m. to 5:00 p.m.	PHYSICAL WORK LOCATION Sacramento, or San Francisco
INCUMBENT (If known)	CURRENT POSITION NUMBER (Agency - Unit - Class - Serial) 680-406-1406-002

YOU ARE A VALUED MEMBER OF THE DEPARTMENT'S TEAM. YOU ARE EXPECTED TO WORK COOPERATIVELY WITH TEAM MEMBERS AND OTHERS TO ENABLE THE DEPARTMENT TO PROVIDE THE HIGHEST LEVEL OF SERVICE POSSIBLE. YOUR CREATIVITY AND PRODUCTIVITY ARE ENCOURAGED. YOUR EFFORTS TO TREAT OTHERS FAIRLY, HONESTLY AND WITH RESPECT ARE IMPORTANT TO EVERYONE WHO WORKS WITH YOU.

BRIEFLY (1 or 2 sentences) DESCRIBE THE POSITION'S ORGANIZATIONAL SETTING AND MAJOR FUNCTIONS:

Under the administrative direction of the Chief Information Officer, the Information Technology Manager II (ITM II) serves as the Chief Information Security Officer (CISO) and manages the agency's information security program which includes but is not limited to formulating long-range programs and objectives, protecting the agency's information technology (IT) and information assets; identify and remediate security gaps; develop, manage and implement information security policies; manage information security incidents and coordinate disaster recovery.

% 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 additional sheet if necessary)*

Business Domain: Information Security Engineering

ESSENTIAL FUNCTIONS:

30% **Security Operations Management**

Provides leadership, direction, and management of the Information Security Office (ISO) personnel. Monitor progress and performance on assignments and take appropriate action to ensure timely and successful completion of activities. Lead the efforts in hiring, developing, and retaining competent and professional personnel to assure an adequate level of specialized analytical and technical security expertise to support current and future needs of the California Public Utilities Commission (CPUC). Oversee development, planning, and training of personnel to support emerging information technology solutions. Maintain current knowledge of security technologies, policies, and standards.

20% **Information Security Strategic Planning, Policies, Governance, Risk, and Compliance**

Manage the Commission's Information Security program. Develop, implement, and maintain information security and privacy policies, standards, guidelines, processes, and procedures in accordance with the department's strategy, State Administrative Manual, State Office of Information Security (OIS) policies and guidance, and other applicable State and federal regulations. Serve as the IT security liaison and CPUC representative with OIS on all IT security matters. Develop an IT security governance and management framework, which aligns with CPUC business goals. Establish cooperative relationships with control agencies, other CPUC Divisions including Legal, Human Resources, data owners, data custodians, and information users. Attend IT security meetings and represent the Commission at the State ISO OIS meetings.

Research, evaluate, and stay apprised of current and new information security technology and trends to develop CPUC's IT security strategic plan and roadmap. Provide guidance for access control using the principle of "least privilege", to CPUC systems and IT assets to ensure that only authorized devices/persons have access as is appropriate in accordance with business needs. Advise senior management and the Chief Information Officer on risk levels and security posture. Collaborate with the Chief Technology Officer, IT infrastructure, and application development teams to ensure security practices properly align and integrate with the system and software development lifecycle and that security requirements including the capture of adequate information for auditing are effectively addressed. Prepare and timely submit reports to control agencies as per OIS schedule.

Develop and implement security strategies and policies that allow CPUC to respond to changing regulatory security requirements/compliances. Create information security initiatives that comply with security requirements that minimize potential threats and security vulnerabilities.

20% **Information Security Program and Risk Management**

Manage the implementation of security controls to effectively protect CPUC's systems and IT assets. Strategically manage the vulnerabilities and threats impacting the CPUC system and information resources; direct the development and implementation of mitigation strategies. Oversee the implementation of an effective IT security risk management program covering risk assessment, mitigation, and evaluation. Lead the preparation and submission of responses related to IT security audit findings, plan actions and milestones to address the findings, and oversee the implementation of planned actions to address the findings. Manage the process to prepare, update and timely submission of Plan of Action and Milestones (POAM) to control agencies. Provide oversight for Technology Recovery Plan (TRP) as per California Department of Technology (CDT) guidelines and lead in the testing and documentation of issues and resolutions. Effectively manage the information security awareness training program for the CPUC.

15%

Security Systems Deployment and Monitoring

Collaborate with the CPUC Network Security and Enterprise Services unit teams to implement and operate industry-strength tools and technologies for endpoint protection, perimeter defense, malware defense, intrusion prevention, and other preventative controls.

10%

Monitor Security Information and Event Management (SIEM) data, review user behavior analytics, manage public key infrastructure (MPKI) certificates, and utilize security and network monitoring tools for data loss prevention (DLP) and endpoint detection and response (EDR). Perform regular security inspections of network, infrastructure, and application systems. Review security processes and cloud computing architectures and provide security recommendations based on control agency security frameworks.

5%

Cyber Security Incident Management and eDiscovery

Develop and implement cyber security resilience strategies to counter, detect, prevent, and contain potential security attacks. Develop, maintain, and test Cyber Incident Response Plan (IRP). Manage security incidents, including investigation, remediation and reporting to control agencies as required. Collaborate with OIS, Cyber Network Defense Team (CND), Computer Crimes Investigative Unit (CCIU), and other law enforcement agencies to investigate and remediate security incident. Manage data searches for CPUC PRA requests, e-Discovery, and computer forensics. Oversee internal technology investigation inquiries and the litigation hold program for the Commission.

MARGINAL FUNCTIONS:

Perform other related duties as required to fulfill CPUC's mission, goals, and objectives. Additional duties may include, but are not limited to, assisting where needed within the ITSD, which may include special assignments

KNOWLEDGE AND ABILITIES **[***From Class Specs***]**

Knowledge of: Principles, practices, and trends of public administration, including management, organization, planning, cost/benefit analysis, budgeting, and project management and evaluation; employee supervision, training, development and personnel management; current computer industry technology and practices; principles of data processing systems design, programming, operations, and controls; State level policies and procedures relating to EDP; the department's goals and policies; department's Affirmative Action Program objectives; a manager's role in the Affirmative Action Program and the processes available to meet affirmative action objectives.

Ability to: Develop and evaluate alternatives, make decisions and take appropriate action; establish and maintain priorities; effectively develop and use resources; identify the need for and assure the establishment of appropriate administrative procedures; plan, coordinate and direct the activities of a data processing staff; make effective use of interdisciplinary teams; reason logically and creatively and use a variety of analytical techniques to resolve managerial problems; present ideas and information effectively, both orally and in writing; consult with and advise administrators and other interested parties on a variety of subject-matter areas, translating technical data processing terms into everyday language; gain and maintain the confidence and cooperation of others; and effectively contribute to the department's affirmative action objectives.

WORK ENVIRONMENT, PHYSICAL OR MENTAL ABILITIES:

- Proficiency with communications-related technologies, including personal computer applications,

telecommunications equipment, Internet, voicemail, email, etc.
- Dress appropriately for a business/government environment.
- Travel to CPUC field offices throughout the state may be necessary. May include overnight or several days stay.
- Work schedule may include evenings and weekends as necessary.

SUPERVISOR'S STATEMENT: ***I HAVE DISCUSSED THE DUTIES OF THE POSITION WITH THE EMPLOYEE***		
SUPERVISOR'S NAME (Print)	SUPERVISOR'S SIGNATURE	DATE

EMPLOYEE'S STATEMENT: ***I HAVE DISCUSSED WITH MY SUPERVISOR THE DUTIES OF THE POSITION AND HAVE RECEIVED A COPY OF THE DUTY STATEMENT***		
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.		
EMPLOYEE'S NAME (Print)	EMPLOYEE'S SIGNATURE	DATE