STATE OF CALIFORNIA CALIFORNIA GAMBLING CONTROL COMMISSION

DUTY STATEMENT

SHADED AREA TO REFLECT RECLASS POSITION NUMBER ONLY

INSTRUCTIONS: Refer to the Essential Functions Duty Statement Manual for instructions on how to complete the Duty Statement.	RPA- **26-004**	EFFECTIVE DATE: **xx/xx/xxxx**

DGS OFFICE OR CLIENT AGENCY	POSITION NUMBER (Agency - Unit - Class - Serial)
California Gambling Control Commission	293-300-1414-002
UNIT NAME AND CITY LOCATED Operations Services Division/Information Technology Unit-Sacramento	CLASS TITLE Information Technology Specialist II – ISO/Privacy/AI Officer
WORKING DAYS AND WORKING HOURS Monday through Friday 8:00 a.m. to 5:00 p.m.	SPECIFIC LOCATION ASSIGNED TO Sacramento
PROPOSED INCUMBENT (If known) NAME	CURRENT POSITION NUMBER (Agency - Unit - Class - Serial) N/A

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.

CALIFORNIA GAMBLING CONTROL COMMISSION MISSION

We are committed to protecting the public by ensuring integrity and justice in the controlled gambling industry through effective regulations and fair application of the law.

COMMITMENT TO DIVERSITY, EQUITY AND INCLUSION

The California Gambling Control Commission (Commission) is committed to building and fostering a diverse workplace. We believe cultural diversity, backgrounds, experiences, perspectives, and unique identities should be honored, valued, and supported. We believe all staff should be empowered. We are proud to foster inclusion and representation at all levels of the Commission.

Under the general supervision of the Chief Information Officer (CIO), the Information Security Officer (ISO) will be responsible for developing Commission polices and directives to conform to State and Federal information security initiatives, Generative Artificial Intelligence and Privacy. The ISO will conduct comprehensive technical analysis on the most complex computer systems process and develop policies and procedures accordingly. The ISO will provide technical strategies to implement enterprise-wide technology policy solutions, write policies and procedures; assist in performing on-going complex assessments on the Commission's enterprise infrastructure, applications and systems to ensure conformity with security/privacy-based industry best practices and standards.

% 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)*
50%	**ESSENTIAL FUNCTIONS:** This position is responsible for analyzing complex processes, State cybersecurity initiatives (California Department of Technology – CDT), developing detailed work plans, analyzing bills and policies, and devising and updating current CGCC policies accordingly. This position will be responsible for assisting with training current CGCC staff in the areas of information policy, procedures, and cybersecurity. **<u>Information Security</u>** • The Commission's ISO will lead the development of information security policies and serve as the information security analyst for statewide information security issues and incidents, and investigations involving external parties such as the Governor's Office, the California Office of Information Security (OIS) and law enforcement agencies. Incumbent will lead the development of the Commission's Information Security, technology recovery, and cyber incident response plans. Incumbent will lead the processes for reporting, logging and coordinating responses to incidents affecting the security of the Commission's resources. Perform internal penetration testing and vulnerability validation of Commission systems, applications, and network environments; document findings, prioritize risks, coordinate remediation measures, and verify corrective actions through retesting and follow-up reporting.

	Risk Analysis • The incumbent will serve as the subject matter expert on the California Department of Technology's Information Security Program Audits and Assessments and the Preliminary Articles Request (PAR) and devise analysis, work plans, policies, procedures and training as required. The incumbent will lead in the preparation and presentation of reports on the security, integrity and availability of information systems. Incumbent will use tools and apply risk methodologies to analyze data and determine risk at technical and business levels. • The Commission's ISO will work with staff to identify appropriate training classes and attend training courses to gain or retain information security skill sets. Incumbent may attend quarterly State Information Security Officer and other security industry specific meetings as required. **ISO Advisory;** • Identify the need for, and provide the CIO by advising, coordinating, developing, overseeing and reviewing information security policies, internal IT and State-level information security policies, practices and procedures. This involves identifying and interpreting State and industry security guidelines, (e.g., the federal NIST CSF controls, SAMM 4800-5300, and related SIMM sections), regulations, and laws governing information and computer systems security. • Coordinate with and advise the Commission's CIO and IT staff on security policies, practices, procedures and processes. • Coordinate and/or oversee major security incidents, events and actions required to resume critical business functions as part of the Commission's security incident response and operational recovery activities. Compile security incident data and prepare and file security incident reports. Identify and recommend security risk mitigation and improvements. • Review, investigate and close-out Security Incident Reports and/or refer security incidents as required for IT and/or policy-based security investigation. • Other information technology duties as required by the CIO such as executing, testing and analyzing information applications particularly with respect to information security issues. • Attends all Commission agendized public meetings/hearings and operates all sound and video equipment either in a backup or primary role.
25%	**Additional Security Architecture, Governance, and CISO Duties** **Security Architecture and Engineering** • Manage security staff and consultants during the System Development Life Cycle (SDLC) for information security deliverables; review, approve, or reject security deliverables throughout each SDLC phase. • Manage the design, documentation, implementation, and continuous operation of security technologies, including SIEM monitoring, endpoint protection and response, intrusion detection and prevention, and data loss prevention to protect sensitive information from theft, misuse, or accidental disclosure. • Collaborate with infrastructure, platform, and application teams to integrate security controls into system design, development, testing, and production deployment. • Review architectural diagrams before and after system changes or enhancements to validate security controls and identify risk. • Manage security testing, including static and dynamic application security testing and penetration testing; review rules of engagement, deployment gates, and test results. • Conduct internal penetration testing, vulnerability assessments, and control validation of Commission systems, networks, applications, and cloud services; document findings, coordinate remediation with technical teams and system owners, track corrective actions through completion, and retest to confirm risks have been mitigated.

	• Configure, update, upgrade and maintain firewalls, operating systems, patching and backups according to best security and privacy standards. • Configure and manage physical security systems according to best security and privacy practices. • Manage and maintain the System Security Plan (SSP) and provide SSP status updates to internal and external oversight bodies upon request. • Ensure security related functional and non-functional requirements are met before systems or components are promoted to production.
15%	**Security Program and Governance** • Set the Commission information security vision, strategy, program objectives, and roadmap aligned with the Commission mission, statewide policies including SAM and SIMM, and federal standards including NIST. • Develop, implement, and maintain information security policies, standards, guidelines, and procedures; ensure consistent governance and enforcement across the Commission. • Serve as the principal security policy liaison with statewide security authorities, including Agency and State CISOs and CDT Office of Information Security; represent the Commission in security matters for boards, task forces, and workgroups as needed. • Lead a comprehensive information security program that includes risk assessment, mitigation, evaluation, and continuous improvement; maintain the risk register and plan of action and milestones, as applicable. • Ensure compliance with applicable federal and California statutes, regulations, policies, standards, and frameworks, including SAM, SIMM, NIST CSF and ISO/IEC as applicable to Commission operations. • Facilitate internal and external security assessments, audits, and technology recovery plan testing; prepare and file required security and recovery reports with control agencies. • Manage progress toward higher maturity levels for Zero Trust Architecture and other statewide cybersecurity initiatives. **Identity, Access, and Data Protection** • Implement and manage Identity and Access Management controls and processes; enforce least privilege and access governance across Commission systems and data. • Conduct periodic reviews of access control, identification and authentication documentation, separation of duties matrices, and related governance artifacts. • Develop security analytics for transactional and access control governance to help detect and prevent fraud, exposure, or inappropriate access through data capture and analysis.
10%	**Incident Response and Technology Recovery** • Maintain the Cybersecurity Incident Response Plan; lead incident response activities including detection, investigation, containment, eradication, recovery, reporting, and post-incident review. • Collaborate with infrastructure and business teams on technology recovery planning and testing to ensure alignment with business continuity programs and statewide requirements. • Responds to building and system alarm calls after hours as required. • Participate in Commission Strategic Plan Projects **Staff Leadership, Training, and Resource Stewardship** • Plan, organize, and direct the workload of security staff, consultants, and project resources; provide project leadership and functional guidance to state staff and contractors.

- Hire, mentor, develop, and retain a high-performing security workforce, as applicable; monitor performance and ensure services are delivered to organizational standards.
- Provide security awareness and training programs for staff and promote a culture of security and accountability.
- Prepare budget estimates and procurement recommendations for security tools and services; optimize operational costs and ensure effective use of resources.

External Coordination and Representation

- Coordinate with control agencies, CDT Office of Information Security, CMD, auditors, law enforcement, regulated entities, counties, vendors, and partner departments; represent the Commission in statewide cybersecurity initiatives, GenAI and privacy.

KNOWLEDGES, SKILLS AND ABILITIES:

Knowledge of: Information technology governance principles and guidelines to support decision making; complex and mission critical business processes and systems; principles, methods and procedures for designing, developing, optimizing, and integrating systems in accordance with best practices; system specifications design, documentation, and implementation methodologies and techniques. Emerging technologies and their applications to business processes; business or systems process analysis, design, testing, and implementation techniques; techniques for assessing skills and education needs to support training, planning and development; business continuity and technology recovery principles and processes; principles and practices related to the design and implementation of information technology systems; information technology systems and data auditing; the department's security and risk management policies, requirements, and acceptable level of risk; application and implementation of information systems to meet organizational requirements; project management lifecycle including the State of California project management standards, methodologies, tools, and processes; software quality assurance and quality control principles, methods, tools, and techniques; research and information technology best practice methods and processes to identify current and emerging trends in technology and risk management processes; and state and federal privacy laws, policies, and standards.

Ability to: Formulate and recommend policies and procedures; perform effectively in a fast-paced environment with constantly changing priorities; establish and maintain project priorities; apply federal, state, department, and organizational policies and procedures to state information technology operations; apply systems life cycle management concepts used to plan, develop, implement, operate, and maintain information systems; positively influence others to achieve results that are in the best interests of the organization; consider the business implications of the technology to the current and future business environment; communicate change impacts and change activities through various methods; conduct end-user training; collaborate closely with technical subject matter experts such as database administrators, network engineers, and server administrators to ensure systems are secure and meet compliance requirements; assess situation to determine the importance, urgency, and risks to the project and the organization; make decisions which are timely and in the best interests of the organization; provide quality and timely ad hoc project information to executives, project team members, and stakeholders; develop decision making documents; and assess and understand complex business processes and customer requirements to ensure new technologies, architectures, and security products will meet their needs. Recognize and apply technology trends and industry best practices; assess training needs related to the application of technology; interpret audit findings and results; implement information assurance principles and organizational requirements to protect confidentiality, integrity, availability, authenticity, and non-repudiation of information and data; apply principles and methods for planning or managing the implementation, update, or integration of information systems components; apply the principles, methods, techniques, and tools for developing scheduling, coordinating, and managing projects and resources, including integration, scope, time, cost, quality, human resources, communications, and risk and procurement management; monitor and evaluate the effectiveness of the applied change management activities; keep informed on technology trends and industry best practices and recommend appropriate solutions;

foster a team environment through leadership and conflict management; effectively negotiate with project stakeholders, suppliers, or sponsors to achieve project objectives; and analyze the effectiveness of the backup and recovery of data, programs, and services.

All employees shall have general qualifications as described by California Code of Regulations, title 2, section 172.

Desirable Experience/Qualifications:

- Familiar with the Government Code and State Administrative Manual sections regarding Information Security and Security Incident Response for California state agencies.
- Knowledge of security principles and practices and the ability to apply technical strategies or solutions.
- The ability to participate in and perform systems analysis, cost/benefit analysis and risk analysis. The incumbent must be able to perform policy analysis related to the Commission's information security needs.
- Knowledge of the Commission's various programs.
- Technical knowledge of the operation and functioning of computers, computer networks and telecommunications links to/from computers.
- Ability to work independently and produce well documented results.
- Ability to communicate with technical and non-technical staff in both verbal and written form.
- Effectively manage changing priorities and able to handle concurrent assignments.
- Ability to show initiative and to work both independently and in a team environment.
- Develop and maintain effective working relationships with business customers, technical staff and co-workers.
- Technical knowledge of computer operating systems.
- Certified Information Systems Security Professional (CISSP) or equivalent experience.
- Experience conducting penetration testing, vulnerability assessments, remediation planning, corrective action tracking, and validation retesting.

SPECIAL PERSONAL CHARACTERISTICS:
Demonstrated ability to act independently, open-mindedness, flexibility, and tact.

SPECIAL REQUIREMENTS:
Limited travel may be required. Occasionally respond after hours and on call.

WORK ENVIRONMENT, PHYSICAL OR MENTAL ABILITIES:

The employee's workstation is located at 2399 Gateway Oaks Drive, Suite 220 and is equipped with standard or ergonomic office equipment, as appropriate. The incumbent works an average of 40 hours per week during normal business hours, however, occasionally some tasks may need to be performed during off hours. This position is a sedentary position; however, there are periods when physical activity in the form of lifting up to 50 pounds of force and in confined quarters due to location of equipment. Office equipment such as computers and telephones are used on a regular basis. Some travel may be required.

This position may be eligible to participate in a hybrid telework schedule. In-office days are required and participation in telework is subject to Commission's Telework policy and supervisor's approval.

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