STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

DUTY STATEMENT

DGS OHR 907 (Rev. 7/2025)

☐ Current
☑ Proposed

RPA NUMBER 30043	DGS DIVISION / OFFICE or CLIENT AGENCY Enterprise Technology Solutions	
UNIT NAME Information Security Office	HEADQUARTER ADDRESS (example: 707 3rd Street, West Sacramento, CA 95605) 707 3rd Street, West Sacramento, CA 95605	
CIVIL SERVICE CLASSIFICATION Information Technology Specialist II	POSITION NUMBER 306-072-1414-XXX	CBID R01
POSITION ELIGIBLE FOR TELEWORK: ☑ Yes ☐ No	PROBATIONARY PERIOD ☐ 6 Months ☑ 12 Months ☐ N/A	WORK WEEK GROUP E
WORK SCHEDULE (DAYS / HOURS) Monday-Friday, 8 AM to 5 PM	TENURE Permanent	
WORKING TITLE Senior Cyber Defense Analyst	TIMEBASE Full Time	
DESIGNATED POSITION FOR CONFLICT OF INTEREST (COI): ☑ Yes ☐ No	BILINGUAL POSITION: ☐ Yes ☑ No LANGUAGE NEEDED: ☐ Verbal ☐ Written Proficiency language in: English	
PROPOSED INCUMBENT (IF KNOWN)	EFFECTIVE DATE	

CORE VALUES / MISSION ☑ Rank and File ☐ Supervisor ☐ Specialist ☐ Office of Administrative Hearings ☐ Client Agency

The Department of General Services (DGS) Core Values and Employee Expectations are key to the success of the Department's Mission. That mission is to "Deliver results by providing timely, cost-effective services and products that support our customers." DGS employees are to adhere to the Core Values and Employee Expectations, and to perform their duties in a way that exhibits and promotes those values and expectations.

POSITION CONCEPT

Under general direction of the Information Technology (IT) Manager I, the IT Specialist II (or Senior IT Specialist) in the Department of General Services, Enterprise Technology Solutions, Security Operations Unit, within the System Engineering and Information Security Engineering domains, serves as the lead subject matter expert for Cloud Security and Enterprise Security Architecture. This position is responsible for designing, implementing, and governing advanced security controls across Microsoft M365, Azure, and Amazon Web Services (AWS) environments. The incumbent leads initiatives for Cloud Security tools integration, Cloud Policy development and enforcement, Policy-as-Code automation, Web Application Firewall (WAF) policy management, vulnerability assessment and mitigation, and attack surface reduction strategies. The role ensures compliance with state and federal regulations, including IRS Pub 1075, HIPAA, and California Civil Code 1798, and provides strategic guidance on risk mitigation for systems containing sensitive data such as FTI, PHI, and PII. This position has elevated access to audit logs, risk assessments, and enterprise security configurations, and plays a critical role in shaping the organization's cloud security posture

SPECIAL REQUIREMENTS

☐ Medical Clearance ☑ Background Clearance ☐ Typing ☐ DMV Pull Notice ☐ Drug Testing
☐ Vehicle Home Storage Permit ☐ Driver's License and Class (specify below in Description) ☐ Certificate (specify below in Description)
☐ Professional License (specify below in Description) ☐ Other (specify below in Description)

Background Clearance
This position and/or location requires background investigation clearance.

Telework
The employee must reside in California.

ESSENTIAL FUNCTIONS

PERCENTAGE	DESCRIPTION
35%	Leads the design, implementation, and governance of cloud security across Microsoft M365, Azure, and AWS environments; Develops and enforces Cloud Security policies, including Policy-as-Code automation, and ensures alignment with enterprise security architecture. Provides expert guidance to ETS management, architects, and vendors on complex security issues to maintain a secure and compliant cloud environment.
20%	Directs vulnerability management lifecycle, including scanning, prioritization, and remediation across cloud and hybrid environments; Implements attack surface reduction strategies and collaborates with system owners to remediate identified risks. Provides executive-level reporting on vulnerability trends and risk posture.
20%	Acts as a lead and expert in administering and optimizing advanced Cloud Security tools (e.g., CSPM, CWPP, SIEM integrations) to monitor and protect enterprise cloud resources; Configures and manages Web Application Firewall (WAF) policies to safeguard critical applications against evolving threats; Oversees integration of security tools with enterprise monitoring and incident response workflows.
20%	Serves as a senior technical advisor for cloud security initiatives; Mentors junior staff and collaborates with cross-functional teams to integrate security best practices into enterprise projects; Represents the Security Operations Unit in strategic planning and governance forums; Ensures compliance with IRS Pub 1075, HIPAA, and California Civil Code 1798 requirements for systems containing sensitive data (FTI, PHI, PII). Conducts risk assessments, develops mitigation plans, and advises leadership on regulatory impacts and security best practices.

MARGINAL FUNCTIONS

PERCENTAGE	DESCRIPTION
5%	Leads independent research and studies and attend job-related educational workshops and trainings in order to maintain professional and technical knowledge of new technologies to ensure the continuing development of solutions that are maintainable, extensible, optimized, and secure.

WORK ENVIRONMENT AND PHYSICAL REQUIREMENTS

☐ Travel (Specify the percentage in the travel box below)

Will be required to report to the office as needed/required.
May be required to respond after hours and on weekends in the event of an emergency.
Professional working environment.

DESIRABLE QUALIFICATIONS

Extensive experience securing Microsoft M365, Azure, and AWS environments. Hands-on experience with Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platforms (CWPP).Proficiency in implementing Policy-as-Code using tools Strong scripting skills (PowerShell, Python, or similar) for automation of security controls. Experience designing and managing WAF policies for enterprise applications. Expertise in vulnerability scanning tools .Ability to develop and execute attack surface reduction strategies across hybrid environments. Deep understanding of IRS Pub 1075, HIPAA, and California Civil Code 1798.Experience conducting risk assessments and implementing compliance frameworks. Ability to design secure architectures for cloud and hybrid environments. Familiarity with Zero Trust principles and NIST cybersecurity frameworks. Strong ability to

lead technical teams and mentor junior staff. Excellent written and verbal communication skills for executive-level reporting and policy development.
Preferred certifications: CISSP, CCSP, AWS Certified Security – Specialty, Microsoft Certified Azure Security Certs

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.

I have discussed these duties with my supervisor and have received a copy of the duty statement. I have read and understand the duties and essential functions listed above and I am able to complete the essential functions with or without a reasonable accommodation. (If you believe you need a reasonable accommodation or you are unsure if you need a reasonable accommodation, please inform the hiring manager and contact the Reasonable Accommodation Unit at reasonableaccommodation@dgs.ca.gov)

EMPLOYEE NAME	EMPLOYEE SIGNATURE	DATE SIGNED

I have discussed the duties of the position with the employee and certify the duty statement represents an accurate description of the essential functions of the position. I have provided the employee with a copy of this duty statement.

SUPERVISOR NAME	SUPERVISOR SIGNATURE	DATE SIGNED

C & P APPROVED BY	DATE SIGNED