PROPOSED

Department of Health Care Access and Information
Duty Statement

Employee Name Vacant	**Organization** Office of Information Services IT Operations Branch Security Operations Group	
Position Number 441-175-1402-XXX	**Location** Sacramento	**Telework Option** Hybrid
Classification Information Technology Specialist I	**Working Title** Security Engineer	

General Description

Under direction, incumbent works under the direction Information Technology Supervisor II, Security Operations Group (SOG). The Information Technology Specialist I (ITS I) works as part of the SOG maintaining the configuration, administration, and monitoring of the SOG's security systems and tools. Identifies and dissects highly targeted attacks and other suspicious activity using a variety of network-based tools. Provides accurate and rapid reporting of in-depth technical analysis results in written form. Research potential exploitation methods. Identifies and analyzes network security appliance logs. Provides mitigation suggestions in the context of a security incidents, as it relates to the technical analysis of PHISHING, Malware, Anti-Virus, or other artifacts. The ITS I works in the Information Security Engineering domain.

Supervision Received	Under direction, incumbent reports to the Information Technology Supervisor II, Security Operations Group.
Physical Demands	Must possess and maintain sufficient strength, agility, endurance, and sensory ability to perform the duties contained in this duty statement with or without reasonable accommodation.
Typical Working Conditions	Requires use of computing devices and phones, frequent face-to-face contact with management, staff, consultants and the public, verbal, written and digital (e-mail) communication, extensive review, analysis and preparation of electronic and written documents, assessment of practical demonstrations, mobility to various areas of the Department, occasional travel and overnight stays to training/conferences or the Los Angeles field office may also be required, and work hours may deviate from core business hours based on the service requirements of the Department.

Job Duties
E = Essential, M = Marginal

35%	E	**Security Engineering** Monitor and assess security controls of information systems on an ongoing basis, documenting changes, conducting security impact analyses, and reporting system security statuses to management. Communicate and collaborate with other technical staff (workstation, system, and network administrators) during incident response and/or meetings. Collaborate with staff to explain and recommend usage capabilities for development of IT policies and procedures. Research, design, and implement improvement to security tools to better protect HCAI assets.

30%	E	**Incident Remediation and Triage** Identify and dissect highly targeted attacks and other suspicious activity using a variety of network-based tools such as network access control and Security Identity and Event Management (SIEM). Provide accurate and rapid reporting to management of in-depth technical analysis results in written form. Research and deep dive into potential exploitation methods such as Phishing and Ransomware. Identify and analyze network security appliance logs. Provide mitigation suggestions in the context of a security incidents, as it relates to the technical analysis of PHSIHING, Malware, Anti-Virus, or other artifacts
20%	E	**Vulnerability Management** Maintain process for hardening of servers, workstations, O365, applications, on-prem tools and other HCAI environments. Conduct vulnerability scans of HCAI systems; conduct ongoing system and account access audits; and respond to external data sources regarding HCAI assets.
10%	E	**Technology Evaluation and Consulting** Research new and emerging network and server technologies and assess the benefit and impact on business operations. Analyze and provide recommendations to executive leadership on opportunities available with Infrastructure as a Service, Platform as a Service, and Software as a Service. Act as HCAI technical representative on multi-departmental task forces, technology forums, advisory committee, etc. that are sponsored by other departments and/or agencies. Participate in the development and implementation of policies and procedures regarding systems, equipment, maintenance, and monitoring. Provide consultation to management, project team members, ISD specialists and business unit representatives on system, network and server technologies and methodologies. Formulate recommendations based on alternative technology solutions. Provide analysis for procurement of network-related software and hardware. Meet with Division customers to determine customer service and technology needs; e.g., service-level agreements and server systems acquisitions and upgrades. Consult with vendors.
5%	M	Perform other related duties as required.

Other Expectations

- Demonstrate a commitment to performing duties in a service-oriented manner.
- Demonstrate a commitment to building an inclusive work environment that promotes HCAI's diversity, equity and belonging where employees are appreciated and comfortable as their authentic selves.
- Demonstrate a commitment to maintaining a work environment free from workplace violence, discrimination, and sexual harassment.
- Demonstrate a commitment to HCAI's mission, vision, and goals.
- Demonstrate a commitment to HCAI's Core Values.
- Maintain good work habits and adhere to all HCAI policies and procedures.

To Be Signed by the Employee and Immediate Supervisor

I have read and understand the duties and expectations of this position

____
Employee Signature/Date

I have discussed the duties and expectations of this position with the employee.

____
Supervisor Signature/Date