DUTY STATEMENT

Employee Name:	
Classification: Information Technology Specialist I	Position Number: 580-152-1402-005
Working Title: Security Operations Center (SOC) Specialist (Information Security Engineering)	Work Location: 1616 Capitol Ave. Sacramento, CA 95814
Collective Bargaining Unit: R01	Tenure/Time Base: Permanent/ Full Time
Center/Office/Division: Information Technology Services Division	Branch/Section/Unit: DCOSB/Security Operations Center

All employees shall possess the general qualifications, as described in California Code of Regulations Title 2, Section 172, which include, but are not limited to integrity, honesty, dependability, thoroughness, accuracy, good judgment, initiative, resourcefulness, and the ability to work cooperatively with others.

This position requires the incumbent to maintain consistent and regular attendance; communicate effectively (orally and in writing) in dealing with the public and/or other employees; develop and maintain knowledge and skill related to specific tasks, methodologies, materials, tools, and equipment; complete assignments in a timely and efficient manner; and, adhere to departmental policies and procedures.

Competencies

The competencies required for this position are found on the classification specification for the classification noted above. Classification specifications are located on the California Department of Human Resource's Job Descriptions webpage.

Job Summary

This position supports the California Department of Public Health's (CDPH) mission and strategic plan by creating innovative solutions, strengthening partnerships and collaborations, and embracing technology. ITSD leverages data and technology to advance goals and inform action and accountability.

Under general direction of the Information Technology Manager I, the Information Technology Specialist I (ITS I) will perform duties in the Information Security Engineering and System Engineering Domains. The ITS I will work as part of the Security Operation Center (SOC) maintaining the conifguration, administration and monitoring of the SOC's security systems and tools. Identify and dissect highly targeted attacks and other suspicious activity using a variety of network-based tools. Provide accurate and rapid reporting of in-depth technical analysis results in written form. Research potential exploitation methods. Identify and analyze network security appliance logs. Review log activity that is not normally detectable through security appliances. 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.

Special Requirements

- ☐ Conflict of Interest (COI)
- ☐ Background Check and/or Fingerprinting Clearance
- ☐ Medical Clearance
- ☐ Travel: Minimal travel to field offices when required
- ☐ Bilingual: Pass a State written and/or verbal proficiency exam in
- ☐ License/Certification:
- ☐ Other:

Essential Functions (including percentage of time)

40% **Incident Remediation and Triage.** Identify and dissect highly targeted attacks and other suspicious activity using a variety of network-based tools. Provide accurate and rapid reporting of in-depth technical analysis results in written form. Research and deep dive into potential exploitation methods. Identify and analyze network security appliance logs. Review log activity that is not normally detectable through security appliances. 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.

25% **Security Engineering.** Monitor and assess security controls of information system 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 I.T. policies and procedures.

25% **Vulnerability Management.** Maintain process for hardening of servers, workstations, O365, on-prem tools and other CDPH environments. Conduct vulnerability scans of CDPH systems; conduct ongoing system and account access audits; and respond to external data sources regarding CDPH assets.

5% **Research and Continuous learning.** Research and evaluate technology releases for hardware and software and make strategic recommendations for systems and equipment that would allow CDPH to meet its information technology goals. Maintain a working knowledge of current information security events and trends. Evaluate system load and projected usage; plan for and make recommendations to ensure system health.

Marginal Functions (including percentage of time)

5% Performs other job-related duties as required. Serve as back-up for peers.

I certify this duty statement represents an accurate description of the essential functions of this position. I have discussed the duties and have provided a copy of this duty statement to the employee named above.		I have read and understand the duties and requirements listed above and am able to perform these duties with or without reasonable accommodation. (If you believe reasonable accommodation may be necessary, or if unsure of a need for reasonable accommodation, inform the hiring supervisor.)	
Supervisor's Name:	Date	Employee's Name:	Date
Supervisor's Signature	Date	Employee's Signature	Date
HRB Use Only: Approved By: Byron Bennett	Date 12/17/20		