GOVERNOR'S OFFICE OF EMERGENCY SERVICES
Exempt Duty Statement - PROPOSED

Title: **Cyber Incident Response Manager**

The California Cyber Security Integration Center (Cal-CSIC) is an integral part of the Governor's Office of Emergency Services' (Cal OES) Homeland Security mission. The Cyber Operations Team is a multi-agency coordination center integrating all aspects of California's cybersecurity mission statewide. The Cyber Operations support the state's Homeland Security strategy through statewide alert monitoring, incident response, root cause analysis, hunting, lab management, and continuous training.

RESPONSIBILITIES:

Under the general direction of the Information Technology Manager II (ITM II), the Cyber Incident Response Manager will provide supervision, direction, focus and oversight of the incident response teams efforts in responding to cyber incidents, resource planning, allocation and completing acquisition requirements for new technologies to support incident response intelligence and mitigation practices. The Cyber Incident Response Manager coordinates with and provides high-level expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents. Responsible for coordinating incident response functions with Cal-CSIC partners and leads activities with entities requesting assistance from the Cal-CSIC. Responsible for writing and publishing after-action reviews. Responds to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities and works with the Cal-CSIC Forensic Lead.

Develops and fosters mentoring/training plans on new incident response technologies to support the Cal-CSIC incident response and post response intelligence activities. Supervises, fosters and mentors team members and conducts training activities. Participates and provides recommendations in resource typing exercises with leadership and various SLTTP agencies to identify requirements to design and develop mutual aid plans.

The Cyber Incident Response Manager will collect data from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within network environments. Uses defensive measures and information collected for the purposes of investigating, analyzing, and responding to cyber incidents with the network environment or enclave. Uses postmortem information from a variety of sources to identify, analyze, and report events that occurred and/or might occur within California, State, Local, Tribal and Territorial and Private entities, with the intent to reduce the likelihood and severity of cybersecurity threats.

Monitors external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense tactics, techniques, threat condition and response, and determine which security issues may have an impact on the enterprise.

Collaborates with the cyber threat intelligence team to create relevant and timely cyber threat products including advisories, recommended actions, and flyers to assist all California and partner entities to include Multi-State Information Sharing and Analysis Center (MS-ISAC), Federal, State, Local, Tribal and Territorial governments, and assists in applying United States Intelligence Community Analytical Standards.

Performs supervisory skills by providing direction, establishing procedures, reviews, and monitors the Cal-CSIC operations performed by other professional staff. Identifies staff needs and provides the necessary training. Evaluates staff performance and takes or recommends appropriate action. Provides overall direction and leadership to meet the programs' strategic goals and business plans.

EXPERIENCE/SKILL REQUIREMENTS:

Possesses a deep level understanding of both Windows, Linux, and networking security. Demonstrable experience using defensive measures (firewalls, IDS/IPS, EDR, etc.) and analysis of security information collected from a variety of sources (packet captures, Windows logs, Linux logs, disk images, memory images, etc.) to identify, analyze, and report events that occur or might occur within the enterprise network.

Understands both offensive and defensive cyber techniques, Mitre Attack Framework, and relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities.

Possesses experience working in state and local fusion centers or cyber intelligence units within federal, state, or local law enforcement agencies highly desired.

Applicant will, at a minimum, possess a valid CompTIA Security+ Certificate or equivalent from an acceptable equivalent source according to industry standards, such as the ISC^2 Systems Security Certified Practitioner. The applicant will also obtain a ISC^2 Certified Information Systems Security Professional (CISSP) within a year of starting.

Must be able to obtain and maintain a Federal **SECRET** clearance.

May have to deploy to remote locations within the state of California in support of incident response for a period of up to one-week with short notice.

DESIRABLE QUALIFICATIONS:

- Effective and persuasive communicator, both orally and in writing, to all levels of officials and the public.
- Excellent analytical and problem-solving skills along with the demonstrated ability for achieving positive results.
- Personal characteristics that include a commitment to teamwork and a collaborative attitude.
- Knowledge of various security methodologies and processes.
- Excellent management skills to direct an experienced professional staff.
- Possess ability to work at speed, under pressure, to make decisions in real time and with reliable accuracy.

OTHER JOB-RELATED DUTIES: The Cyber Incident Response Manager will perform other job-related duties as required to fulfill the Cal OES mission, goals and objectives. Additional duties may include, but are not limited to: (a) assisting where needed within the program, which may include special assignments; (b) complying with general State and Cal OES administrative reporting requirements (i.e. completion of time sheets, project time reporting, travel requests, travel expense claims, work plans, training requests, individual development plans, etc.); (c) attending staff meetings and/or conducting or attending training; (d) supporting the Cal-CSIC Operations; (e) performing after-hours duty officer function in rotation with members of STAC staff.