State of California
GOVERNOR'S OFFICE OF EMERGENCY SERVICES

POSITION DUTY STATEMENT

BU: 1, 4, 9, 10, 11, 12 & 14

EMPLOYEE:	CLASS TITLE: INFORMATION TECHNOLOGY SPECIALIST III **Cyber Defense Incident Responder**	HEADQUARTERS: Mather Campus
PROGRAM/UNIT: Homeland Security Division (HSD) / California Cybersecurity Integration Center (Cal-CSIC)	POSITION/ CONTROL NUMBER: **375-1415-006 61450**	CBID: M01
TENURE: Perm	TIME BASE: Fulltime	WORK WEEK GROUP: E
APPT EFFECTIVE DATE:	Range (If Applicable)	PROBATIONARY PERIOD: ☐ 6 Mos. ☒ 12 Mos. ☐ N/A
IMMEDIATE SUPERVISOR:	CONFLICT OF INTEREST CATEGORY: ☒ Yes ☐ No	DMV PULL PROGRAM: ☒ Yes ☐ No

1. SUPERVISION RECEIVED: The information Technology Specialist is under the direct supervision of the Incident Response Branch Chief, ITM-II.

2. SUPERVISION EXERCISED: N/A

3. PHYSICAL DEMANDS (SEE ADDITIONAL PAGES)
   Appropriate business attire for a professional office environment; ability to sit in a normal seated position for extended periods; ability to effectively handle multiple tasks and changing priorities.

4. PERSONAL CONTACT (WHO THE EMPLOYEE MAY BE IN CONTACT WITH WHILE PERFORMING DUTIES):
   This incumbent will have regular contact with Cal OES executive staff, peers, subordinates, other employees of Cal OES, governmental agencies, including but not limited to federal agencies, private nonprofit (PNP) organizations, the Legislature, Department of Finance and the Governor's Office.

5. ACTIONS AND CONSEQUENCES (AS RELATED TO DUTIES PERFORMED):
   Failure to effectively perform the duties of the position will result in the agency's inability to ensure consistency and compliance with state and federal law, regulation, policies, plans and procedures. This could result in statewide impacts, including, but not limited to, loss of state and federal disaster assistance funding for Cal OES, other state agencies, local agencies, PNP organizations, individuals and businesses impacted by disasters, regulatory compliance, and negative audit findings for Cal OES.

6. EMERGENCY OPERATIONS – ACTIVATION/OPERATIONAL ASSIGNMENT 100%:
   When requested to fill an operational assignment and until demobilized, the following duties will be performed, and your regular duties may temporarily cease:

   May be required to work in the State Operations Center (SOC), Regional Emergency Operations Center (REOC), Joint Field Office (JFO), Area Field Office (AFO), Local Assistance Center (LAC), or other location to provide assistance in emergency response and recovery activities. All staff is required to complete operational related training and participate in one of three Readiness Teams that rotate activation availability on a monthly basis if not assigned to an Operational Branch (e.g., Fire/Law/Region/PSC Operations (Technicians)/PSC Engineering (Engineers). May be required to participate in emergency drills, training and exercises.

CONTINUED:

Staff need to work effectively under stressful conditions; work effectively & cooperatively under the pressure of short leave time; work weekends, holidays, extended and rotating shifts (day/night). Statewide travel may also be required for extended periods of time and on short notice.

While fulfilling an operational assignment it is important to understand that you are filling a specific "position" and that position reports to a specific Incident Command System (ICS) hierarchy. This is the chain of command that you report to while on this interim assignment.

On Call/Standby/Duty Officer (if applicable)

If assigned on-call, standby or as a Duty Officer, you are required to be ready and able to respond immediately to any contact by Governor's Office of Emergency Services (Cal OES) Management (including contact from the State of California Warning Center) and report to work in a fit and able condition if necessary as requested.

7. JOB DESCRIPTION/GENERAL STATEMENT:

Under the general supervision of the Incident Response Branch Chief, receiving general direction from the Senior Cyber Defense Incident Responder of California Cybersecurity Integration Center, the Cyber Defense Analyst will work within the California Cybersecurity Integration Center (Cal-CSIC) and with OES partner analysts to identify, collect and perform analysis of raw, primary and secondary data derived from various sources. The incumbent will perform and provide guidance on methods to investigate, document, and report on cybersecurity issues and emerging trends, provide actionable technical and tactical cyber information and intelligence to federal, state, local, tribal, and territorial (SLTT) governmental and private sector partners through ad hoc reports, briefings and presentations. The incumbent works with the analyst team to create relevant and timely cyber threat products including advisories, recommended actions, and bulletins to assist California and partner entities to include Multi-State Information Sharing and Analysis Center (MS-ISAC), federal and SLTT personnel, and assist in applying prescribed analytical standards.

Percent of Time	**ESSENTIAL FUNCTIONS**
45%	Provide direction and focus to the incident response teams efforts in resource planning, allocation and completing the requirements for acquisition. Coordinate with and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents. Coordinate incident response functions. Write and publish 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.
30%	Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise. Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
20%	Coordinates with the Cyber Defense Incident Responder concerning crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Acts as a member of a tactical incident response team deployable to various locations within the state of California in direct support of incident response efforts as outlined by Government Code 8586.5. Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies.

Percent of Time	**MARGINAL FUNCTIONS**
5%	Other Related Duties as Required The incumbent will perform other related duties as required to fulfill the Cal OES mission, goals and objectives. Additional duties may include, but not be 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.); and (c) attendance at staff meetings.

KNOWLEDGE, SKILLS, AND ABILITIES

Ability to analyze malware.
Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.
Ability to interpret the information collected by network tools (e.g. Nslookup, Ping, and Traceroute).
Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.
Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
Skill in developing and deploying signatures.
Skill in detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort).
Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.
Skill in evaluating the adequacy of security designs.
Skill in using incident handling methodologies.
Skill in using protocol analyzers.
Skill in collecting data from a variety of cyber defense resources.
Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
Skill in reading and interpreting signatures (e.g., snort).
Skill in assessing security controls based on cybersecurity principles and tenets. (e.g., CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.).
Skill in performing packet-level analysis.
Skill in recognizing vulnerabilities in security systems. (e.g., vulnerability and compliance scanning).
Skill in conducting trend analysis.
Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
Skill to use cyber defense Service Provider reporting structure and processes within one's own organization.
Knowledge of computer networking concepts and protocols, and network security methodologies.
Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
Knowledge of cybersecurity and privacy principles.
Knowledge of cyber threats and vulnerabilities.
Knowledge of specific operational impacts of cybersecurity lapses.
Knowledge of authentication, authorization, and access control methods.
Knowledge of cyber defense and vulnerability assessment tools and their capabilities.
Knowledge of computer algorithms.
Knowledge of encryption algorithms
Knowledge of cryptography and cryptographic key management concepts
Knowledge of database systems.
Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).
Knowledge of vulnerability information dissemination sources (e.g., alerts, advisories, errata, and bulletins).
Knowledge of incident response and handling methodologies.
Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.
Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
Knowledge of network access, identity, and access management (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).

Knowledge of network traffic analysis methods.
Knowledge of new and emerging information technology (IT) and cybersecurity technologies.
Knowledge of operating systems.
Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).
Knowledge of policy-based and risk adaptive access controls.
Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
Knowledge of key concepts in security management (e.g., Release Management, Patch Management).
Knowledge of security system design tools, methods, and techniques.
Knowledge of telecommunications concepts (e.g., Communications channel, Systems Link Budgeting, Spectral efficiency, Multiplexing).
Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organization.
Knowledge of Virtual Private Network (VPN) security.
Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.
Knowledge of Insider Threat investigations, reporting, investigative tools and laws/regulations.
Knowledge of adversarial tactics, techniques, and procedures.
Knowledge of network tools (e.g., ping, traceroute, nslookup)
Knowledge of defense-in-depth principles and network security architecture.
Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).
Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).
Knowledge of interpreted and compiled computer languages.
Knowledge of collection management processes, capabilities, and limitations.
Knowledge of front-end collection systems, including traffic collection, filtering, and selection.
Knowledge of cyber defense and information security policies, procedures, and regulations.
Knowledge of the common attack vectors on the network layer.
Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).
Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).
Knowledge of system administration, network, and operating system hardening techniques.
Knowledge of applicable laws, statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures.
Knowledge of cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.
Knowledge of encryption methodologies.
Signature implementation impact for viruses, malware, and attacks.
Knowledge of Windows/Unix ports and services.
Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).
Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).
Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities.
Knowledge of Personally Identifiable Information (PII) data security standards.
Knowledge of Payment Card Industry (PCI) data security standards.
Knowledge of Personal Health Information (PHI) data security standards.

Knowledge of systems security testing and evaluation methods.
Knowledge of countermeasure design for identified security risks.
Knowledge of network mapping and recreating network topologies.
Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).
Knowledge of the use of sub-netting tools.
Knowledge of operating system command-line tools.
Knowledge of embedded systems.
Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.
Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
Knowledge of how to use network analysis tools to identify vulnerabilities.
Knowledge of penetration testing principles, tools, and techniques.
Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)

REQUIRED QUALIFICATIONS

Applicant will, at a minimum, possess a valid SANS GIAC Security Essentials or equivalent from an acceptable equivalent source according to industry standards, such as the ISC^2 Systems Security Certified Practitioner.

DESIRED QUALIFICATIONS

Other desired certifications include the GCED: GIAC Certified Enterprise Defender or equivalent, the GCIA: GIAC Certified Intrusion Analyst or equivalent or the GMON: GIAC Continuous Monitoring Certification or equivalent
Knowledge of the state and related federal laws, rules, regulations, policies and procedures is desirable.

ADDITIONAL REQUIREMENTS

Must exercise good writing skills; follow oral and written directions, be responsive to the needs of the public and employees of Cal OES and other agencies; analyze situations and take effective action using initiative, resourcefulness, and good judgment.

May need to work with limited supervision. Consistent with good customer service practices and the goals of the Cal OES Strategic Plan, the incumbent is expected to be courteous and provide timely responses to internal and external customers, follow through on commitments, and solicit and consider internal and external customer input when completing work assignments.

Incumbent will be working in a classified office environment. This necessitates pulling open a metal vault door; requires approximately 30 lbs. of pull to open the door for access.

Incumbent shall obtain a SECRET level security clearance within six months of hire date and maintain the clearance as a condition of employment.

The incumbent will have to operate a government vehicle (sedan to van) as part of their duties to support incident response activities as well as occasional administrative requirements.

PHYSICAL AND MENTAL REQUIREMENTS OF ESSENTIAL FUNCTIONS					
Activity	**Not Required**	**Less than 25%**	**25% to 49%**	**50% to 74%**	**75% or More**
VISION: Reviewing mail; preparing various forms; proofreading documents; reading printed material, computer screens, and handwritten materials.	☐	☐	☐	☐	☒
HEARING: Answering telephones; receiving verbal information from outside sources; understanding verbal instruction.	☐	☐	☐	☐	☒
SPEAKING: Receiving visitors; answering inquiries and providing verbal information or instruction.	☐	☐	☐	☐	☒
MOVEMENT: Delivering material to others; picking up materials from others; copying; faxing; distributing information; filing.	☐	☒	☐	☐	☐
SITTING: At a computer terminal or desk; conferring with employees.	☐	☐	☐	☒	☐
STANDING:	☐	☒	☐	☐	☐
BALANCING:	☐	☐	☐	☐	☒
CONCENTRATING: Reviews and reads records/documents, researches, composes, analyzes, compiles, and updates technical documents; multi-tasking; prepares various forms and documents.	☐	☐	☐	☐	☒
COMPREHENSION: Understanding needs of co-workers, clients; understands procedures and practices; Understands laws, regulations related to their work.	☐	☐	☐	☐	☒
WORKING INDEPENDENTLY: Possesses ability to work independently as well as a team member, have good interpersonal and communication skills, ability to follow directions, take initiative, assume responsibility, and exercise good judgment and tact. Must be able to work alone without much guidance or interaction or interaction from other staff.	☐	☐	☐	☒	☐
LIFTING UP TO 10 LBS. OCCASIONALLY:	☐	☐	☒	☐	☐

PHYSICAL AND MENTAL REQUIREMENTS OF ESSENTIAL FUNCTIONS					
Activity	**Not Required**	**Less than 25%**	**25% to 49%**	**50% to 74%**	**75% or More**
LIFTING UP TO 20 LBS. OCCASIONALLY AND/OR 10 LBS. FREQUENTLY:	☐	☒	☐	☐	☐
LIFTING UP TO 20-50 LBS. OCCASIONALLY AND/OR 25-50 LBS. FREQUENTLY:	☐	☒	☐	☐	☐
FINGERING: Pushing buttons on telephone; typing; copying.	☐	☐	☐	☐	☒
REACHING: Answering phones.	☐	☐	☒	☐	☐
CARRYING: Distributing mail; reports; stocking supplies.	☐	☒	☐	☐	☐
CLIMBING: stairs	☐	☒	☐	☐	☐
BENDING AT WAIST:	☐	☐	☐	☐	☒
KNEELING:	☐	☒	☐	☐	☐
PUSHING OR PULLING:	☐	☒	☐	☐	☐
HANDLING: Documents, manuals	☐	☐	☐	☐	☒
DRIVING:	☐	☒	☐	☐	☐
OPERATING EQUIPMENT: Computer; telephone; copy machine; fax.	☐	☐	☐	☐	☒
WORKING INDOORS:	☐	☐	☐	☐	☒
WORKING OUTDOORS:	☐	☒	☐	☐	☐
WORKING IN CONFINED SPACE: Enclosed office environment.	☐	☐	☐	☐	☒

OTHER INFORMATION

Must have knowledge of the state and related federal laws, rules, regulations, policies and procedures. Must exercise good writing skills; follow oral and written directions, be responsive to the needs of the public and employees of Cal OES and other agencies; analyze situations and take effective action using initiative, resourcefulness, and good judgment. May need to work with limited supervision.

Consistent with good customer service practices and the goals of the Cal OES Strategic Plan, the incumbent is expected to be courteous and provide timely responses to internal and external customers, follow through on commitments, and solicit and consider internal and external customer input when completing work assignments.

SIGNATURES

Certification of Applicant/Employee

Note – If any concerns with performing the duties of this position with or without reasonable accommodation, discuss your concerns with the hiring supervisor, who in turn, will discuss with the Reasonable Accommodation Coordinator.

I certify that I possess essential personal qualifications including integrity, initiative, dependability, good judgment, and ability to work cooperatively with others; and a state of health consistent with the ability to perform the assigned duties as described above with or without reasonable accommodation.

I have read and discussed these duties with my supervisor:

_____ _____

Employee's Signature *Date*

I certify that the above accurately represents the duties of the position:

_____ _____

Supervisor's Signature *Date*

_____

Civil Service Title