State of California
GOVERNOR'S OFFICE OF EMERGENCY SERVICES
POSITION DUTY STATEMENT
BU: 1 and Non-Represented

EMPLOYEE	**CLASS TITLE:** Information Technology Specialist III **WORKING TITLE:** Senior Cyber Defense Forensics Analyst	**HEADQUARTERS:** Mather Campus
PROGRAM/UNIT: Homeland Security/ California Cybersecurity Integration Center (Cal-CSIC)/ Cyber Operations Branch	**POSITION NUMBER:** 163-420-1415-007 (12039)	**CBID:** M01
TENURE: Permanent	**TIME BASE:** Full Time	**WORK WEEK GROUP**: E
APPT. EFFECTIVE DATE:	**RANGE (IF APPLICABLE):** N/A	**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 III, Senior Cyber Defense Forensics Analyst receives administrative direction from the Information Technology II (ITM II), Cyber Operations Branch Chief; however, direction and assignments may also come from the Cyber Incident Response Manager, Forensics Lead, or California Cybersecurity Integration Center (Cal-CSIC) Commander, when designated.

2. SUPERVISION EXERCISED:
None, but may serve in a lead capacity over a cross-functional team consisting of members from the Cal-CSIC and other partner agencies.

3. PHYSICAL DEMANDS (SEE ADDITIONAL PAGES):
Frequent sitting for long periods of time in an office-setting environment with the use of a telephone and personal computer. 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. This position requires the ability to work under pressure to meet deadlines and may require excess hours to be worked. Occasional travel may be required.

4. PERSONAL CONTACT (WHO THE EMPLOYEE MAY BE IN CONTACT WITH WHILE PERFORMING DUTIES):
The incumbent will have daily contact with a variety of individuals, including California Governor's Office of Emergency Services (Cal OES) staff, representatives from state and federal agencies (i.e., Department of Technology, Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) from both public and private sectors), consultants, vendors, local government officials, and private non-profit organizations representatives.

5. ACTIONS AND CONSEQUENCES (AS RELATED TO DUTIES PERFORMED):
This position requires a thorough understanding of the roles, responsibilities, and objectives of the unit, as well as the goals and objectives of Homeland Security and the department. The consequence of error in the context of reviewing current cyber threat landscape and lending expertise to help external customers/clients understand its security posture can be signification. Failure to effectively perform the duties of this position may result in the department's inability to ensure consistency and compliance with applicable state and federal laws, rules, and regulations related to IT cyber security and analysis. The consequence of poor decision, judgment or advice, or inadequate research may have a negative or serious impact on the reputation of the Cal-CSIC and customer confidence levels.

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:

(CONTINUED) EMERGENCY OPERATIONS – ACTIVATION/OPERATIONAL ASSIGNMENT 100%:
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.

Staff need to work efficiently under stressful conditions and collaborate effectively under the pressure of short notice leave; 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 (as 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 Cal OES Management (including contact from the California Warning Center) and report to work in a fit and able condition if necessary, as requested.

7. JOB DESCRIPTION/GENERAL STATEMENT:
The Cyber Operations Branch is a proactive and dynamic team dedicated to providing exceptional cybersecurity services to external customers and clients of California. Our team enables Cal OES to achieve its mission by providing governance, oversight, and support of operational resiliency and asset safeguards in a relevant, timely, and data-driven manner. We specialize in incident response, threat identification, containment, and eradication, utilizing rapid response tactics to mitigate potential cyber threats. Our team also offers proactive security assessments, including network perimeter vulnerability scans, dark web reviews, net flow traffic analysis, and a free 30-day license for an endpoint detection and remediation tool. Additionally, our digital forensics capabilities include hard disk forensics, memory forensics, network forensics, and malware analysis. With our expertise and methodology, we help our clients make informed decisions about where to invest their resources to address the highest priority cyber risks unique to their business goals and operations.

Under the administrative direction of the Information Technology Manager II (ITM II) over the Cyber Operations Branch, the Information Technology Specialist (ITS III) serves as the Senior Cyber Defense Forensics Analyst. This mastery-level position is responsible for leading a team of Cyber Analysts providing critical cybersecurity services to external customers and partners and serving as the primary consultant in cybersecurity forensics and incident response. The Senior Cyber Defense Forensics Analyst works within the Cal-CSIC and with Cal OES partner analysts to identify, collect and perform analysis of raw, primary, and secondary data derived from various sources. The role focuses on delivering incident response, threat identification, and security assessments to a diverse range of clients including federal, state, local, tribal, and territorial (SLTT) governmental entities and private sector partners. Key responsibilities include but are not limited to, analyzing data from various sources to identify cyber threats, conducting forensic investigations, and producing actionable intelligence for external stakeholders. The successful incumbent will create and disseminate cyber threat products, including advisories and bulletins, to assist California's partners and entities such as the Multi-State Information Sharing and Analysis Center (MS-ISAC).

This senior-level position requires expertise in advanced cybersecurity, digital forensics, and incident response, typically acquired through years of experience in IT and cybersecurity leadership roles. The successful candidate will serve as a key strategic partner to various state departments, agencies, and external organizations, spearheading efforts to enhance cybersecurity resilience across California's public and private sectors.

(CONTINUED) JOB DESCRIPTION/GENERAL STATEMENT:
The ITS III will collaborate with security teams, vendors, and partner agencies to develop, implement, and oversee cybersecurity strategies, comprehensive incident response plans, and threat mitigation solutions. Critical to this role is the ability to stay abreast of emerging cybersecurity technologies, advanced forensic techniques, and evolving threat landscapes. Adherence to applicable federal and state laws, rules, and regulations is paramount, including but not limited to the State Administrative Manual (SAM) 5300 requirements and relevant NIST frameworks. The ITS III must demonstrate the ability to interpret and apply these regulations in the context of large-scale, multi-agency cybersecurity efforts.

This role requires exceptional leadership skills, the ability to communicate complex technical concepts to stakeholders, and a proven track record in managing cybersecurity projects and incident responses across diverse organizational environments. The Senior Cyber Defense Forensics Analyst demonstrates team leadership skills within a team setting and models the department's values. This position requires the incumbent to be a skilled communicator and team player, using cyber forensics expertise, incident response, and threat analysis to break down complex security concepts for diverse audiences.

Percent of Time	ESSENTIAL FUNCTIONS
40%	**CYBERSECURITY INCIDENT RESPONSE AND FORENSIC ANALYSIS SERVICES** Serves as the technical lead, providing expert guidance, training, and support to the incident response teams serving various state departments, agencies, and external partners. Develops strategic direction for incident response efforts, focusing on resource planning and allocation to meet diverse client needs across California's public and private sectors. Coordinates with and provides expert technical support to cyber defense technicians/representatives across multiple agencies and organizations to resolve complex cyber defense incidents affecting external stakeholders. Leads and coordinates multi-agency incident response functions, ensuring seamless collaboration between Cal OES and its partner organizations. Responsible for authoring and publishing comprehensive after-action reviews for client organizations, detailing forensic analyses and providing actionable recommendations. Manages the response to critical cybersecurity events impacting external clients, using innovative strategies to shield their systems and information from harm and ensure their ongoing security. Conducts in-depth investigations of cybersecurity incidents for partner agencies and organizations, performing advanced forensics analysis and creating detailed reports for stakeholders. Develops and delivers specialized training programs for cybersecurity professionals across various public/private organizations. Provides mentorship and technical guidance to cybersecurity teams in multiple agencies, to enhance the overall cyber defense capabilities of California's public and private sectors.
30%	**CYBERSECURITY STRATEGY AND SUPPORT** Designs and oversees the development and implementation of advanced cyber defense system architectures and solutions across multiple platforms for external partner agencies, local governments, and critical infrastructure sectors. Develops high-level cyber defense policies, requirements, and methodologies tailored to the specific needs of various external clients, including state departments, local governments, and private sector partners. Leads deployable tactical incident response teams to various locations within California, providing expert-level support to external agencies during critical cybersecurity incidents, as per Government Code 8586.5. Prepares and disseminates comprehensive cyber defense techniques, guidance, and strategic reports on incident findings for stakeholders, including partner agencies and organizations. Delivers executive-level presentations and briefings to leadership of partner agencies, local governments, and private sector organizations on complex cyber defense concepts and strategies. Coordinates cyber defense infrastructure design, modification, and implementation for multiple external partners, aligning with their specific security needs and statewide cybersecurity objectives. Collaborates with key partners in development and implementation of technical cyber defense policies, procedures, requirements, and methodologies that can be adopted by external agencies and partners across various sectors. Provides strategic direction to external partners during cyber crises, collaborating with their incident response teams to mitigate immediate and potential threats. Leads the evaluation and integration of emerging technologies into existing cyber defense architectures for partner agencies and critical infrastructure organizations.

20%	**CYBERSECURITY CONSULTING AND THREAT INTELLIGENCE SERVICES** Continuously monitors external data sources, including cyber defense vendor sites, Computer Emergency Response Teams, and Security Focus, to maintain up-to-date threat intelligence relevant to Cal-CSIC's external customers and partners. Analyzes and disseminates timely threat intelligence reports to public and private sector entities, helping them understand potential impacts on their enterprises. Develops and recommends proactive cybersecurity policies, procedures, and methodologies tailored to the specific needs of partner agencies and external organizations. Provides expert consultation on the implementation of advanced cybersecurity tools and programs, such as Endpoint Detection and Response solutions, for external clients. Assists partner agencies and private sector entities in developing multi-departmental cybersecurity systems, ensuring integration and compliance across diverse organizational structures. Provides guidance on compliance with cybersecurity policies and requirements, including NIST 800-53 and State Administrative Manual (SAM) 5300, offering recommendations and best practices, to help external customers improve their cybersecurity posture. Coordinates vulnerability assessments across multiple client environments, tracking and reporting on vulnerability statuses to enhance overall cybersecurity posture. Analyzes and validates security alerts from various sources for external partners, distinguishing between malicious and benign activities to reduce false positives and enhance threat detection accuracy. Develops and maintains comprehensive documentation of cybersecurity policies, procedures, and best practices for use by external agencies and organizations. Provides strategic direction on continuous monitoring and analysis of system activities for partner entities, recommending adherence to relevant policies and procedures.
5%	**PROFESSIONAL DEVELOPMENT** Serves as a subject matter expert and thought leader in cybersecurity, actively contributing expertise to the Cal-CSIC's overall strategic planning and policy development. Leads and facilitates professional development initiatives across the Cal-CSIC, including organizing and conducting training sessions/workshops on cybersecurity topics. Collaborates closely with the IT division to align cybersecurity strategies with broader technological initiatives. Represents the Cal-CSIC at industry-level conferences, forums, and interagency meetings, sharing insights and best practices while also bringing back valuable knowledge to enhance organizational capabilities. Mentors junior staff members within the Cyber Operations Branch and the Cal-CSIC. Actively participates in and leads professional internal meetings, contributing insights and fostering collaboration between different units and departments. Maintains expertise in the latest trends, tools, and methodologies in cybersecurity, threat intelligence, and incident response. Performs special assignments or projects, including leading or participating in other related initiatives.
Percent of Time	**MARGINAL FUNCTIONS**
5%	**OTHER JOB-RELATED DUTIES AS REQUIRED** Performs other job-related duties as required to fulfill Cal OES's mission, goals and objectives. Additional duties may include but are not limited to: (a) assisting where needed within the department and program, which may include special assignments; public speaking; (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.

ADDITIONAL INFORMATION

Must have a valid Driver's License and is required to participate in the Department of Motor Vehicles' Pull Notice Program.

HOMELAND SECURITY SPECIAL REQUIREMENTS:

Access to Federal Security Information is required for this position. Pursuant to this requirement, incumbents must be eligible for and apply for a Federal Department of Homeland Security (DHS) SECRET-level security clearance upon hire and once granted, maintain the clearance as a condition of employment.

The ideal candidate for this position should possess the following preferred skills and qualifications:

- Cyber Security Certifications: Highly desired certifications include GIAC Certified Forensic Analyst (GCFA) and GIAC Security Essentials (GSEC), demonstrating a strong foundation in cybersecurity principles and practices.
- Senior-Level Security Certifications: Certified Information Systems Security Professional (CISSP) or Certified Information Security Manager (CISM), showcasing comprehensive understanding of information security management.
- Expert-level understanding: Comprehensive knowledge of cybersecurity laws, regulations, policies, ethics, and privacy at both state and federal levels, with the ability to interpret and apply these in complex scenarios.
- Advanced networking and security architecture expertise: In-depth knowledge of enterprise-level computer networking, security architectures, and the ability to design and implement robust cyber defense systems.
- Leadership and project management skills: Demonstrated ability to lead teams, manage complex projects, and coordinate multi-agency efforts in cybersecurity initiatives.
- Advanced incident response experience: Proven track record in managing and resolving complex, large-scale cyber incidents across multiple sectors or agencies.
- Interpersonal skills: Exceptional interpersonal skills are required to build strong relationships and communicate effectively.
- California state government knowledge: Familiarity with the functions and organizations of California state government is preferred.
- Handling sensitive material: The ability to work with sensitive material, maintain confidentiality, and adhere to strict security protocols is essential.

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.	☐	☐	☐	☐	☒

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 10 LBS. OCCASIONALLY:	☐	☒	☐	☐	☐
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 and materials.	☐	☐	☐	☐	☒
DRIVING:	☐	☒	☐	☐	☐
OPERATING EQUIPMENT: Computer; telephone; copy machine; fax.	☐	☐	☐	☐	☒
WORKING INDOORS: Office Setting.	☐	☐	☐	☐	☒
WORKING OUTDOORS:	☐	☒	☐	☐	☐
WORKING IN CONFINED SPACE:	☐	☒	☐	☐	☐

OTHER INFORMATION

Must have knowledge or ability to become familiar with 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 Cal OES's Strategic Plan, and the California Homeland Security Strategy, 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