State of California, Military Department

State Active Duty (SAD)

Vacancy Announcement

1 Position Available (TEMP)

Position Details

Announcement Number:	SAD VA 2024-035
Opening Date:	2 May 2024
Closing Date:	8 May 2024
Position Title:	Cyber Defense Analyst (SAD E-7/CW2/O-3)
Duty Location:	JRIC/Cal-CSIC, Norwalk, CA
Selecting Official:	OIC Knowledge Manager, Cyber Cal-CSIC
Projected Employment Date:	15 May 2024

Vacancy Announcement Details

The California Military Department is accepting applications for the State Active-Duty position indicated above. **Current SAD employees will have priority for hire.** An appointment to this position provides full benefit status for the appointee and their beneficiaries. The incumbent will be appointed on annually renewable State Active-Duty orders through year six, at which time the incumbent may be eligible for career status IAW CMD Reg 600-1, dated 21 April 2020. Continuation and subsequent extensions of service will be determined by the individual's performance of duty and continuation of funding. **The service member selected for this position will be paid at their federal or California State Guard pay grade, not to exceed E-7/CW2/O-3.** This announcement has minimum requirements. Failure to meet these requirements will cause your application to be rejected from consideration. While it is important for you to read the entire announcement closely, please pay particular attention to the instructions at the end of this announcement for documents required to submit a complete application. **Applications missing signatures and required documents will not be considered.** The Service Member selected for this position may be eligible for health, dental, vision and life insurance benefits. Other benefits may also be available to those who qualify such as Service Member Assistance Programs, Group Legal Services, Long-Term Disability Insurance, Long-Term Care Insurance, Retirement Annuity, Supplemental Investment, and the Military Service Buy Back Program. **Reimbursement for moving and relocation expenses will not be paid.**

Eligibility Requirements

- Active members of the California Military Department (Army, Air, CSG) in the grades **E-6 through E-8 or WO1 through CW3 or O-1 through O-4** may apply. Applicants must have a military affiliation per Para 3-2 of CMD Reg. 600-1. CSG members who have no prior federal military experience must be a member of the CSG in good standing for a minimum of two years for eligibility for SAD vacancies. **CSG members must submit a copy of their CSG orders with their application.** .
- Must possess, at minimum, a security clearance.
- For CSG personnel, the medical readiness and physical fitness verification memorandum endorsed by the CSG unit commander must be submitted with the application.
- Completion of military and civilian education (high school or equivalent) requirements commensurate with the grade of the applicant are required. **Attach documentation of your highest level of civilian education.**
- Military assignments appropriate to the grade of the applicant are required.

- Required to meet height/weight and physical fitness standards prescribed by their military branch of membership.
- Applicants must meet, and maintain, federally recognized medical fitness standards. **Attach a current copy, within the past twelve months of your military component's verification of these requirements. (See instructions at the end of this announcement for required component-specific documents).**
- Appropriate military uniform with federally recognized, or CSG recognized, rank will be worn in accordance with military regulation.
- Must be able to pass both State and Federal background checks (Live Scan). Continuation of employment is contingent upon maintaining favorable State and Federal background checks.
- Must possess a valid state driver's license. **Attach a current copy, within the past six months of your Department of Motor Vehicle's printout.**

Primary Duties and Responsibilities

OPCON:
Cal-CSIC Commander
Cal-CSIC Cyber Threat Intel Branch Chief

ADCON:
Chief of Cyber Operations CMD
Cal-CSIC ADCON OIC/NCOIC

- Supervised by the California Office of Emergency Services, Cyber Security Integration Center (Cal-CSIC), Cyber Operations Branch Chief, or designee.
- The Cyber Operations Branch Chief, or designee, will provide day-to-day supervision, assignment of work schedule and validation of hours worked by the employee.
- The JRIC Director, or designee, may task the analyst up to 25% of the time.
- Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network to protect information, information systems, and networks from threats.
- Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
- Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.
- Serves as a Cal-CSIC cyber operations team member and a liaison to the JRIC to assist with cyber incident response activities impacting the state of CA, JRIC AOR, local, tribal, and territorial governments.
- Serves as a point of contact for subject matter material for the JRIC AOR.
- Ensures appropriate relationships are made at the Federal, State, and local levels for information sharing and coordination activities.
- Works to advance joint, analytical, and collaborative opportunities with new and existing Cal CSIC partners.
- Briefs on cyber incident response activities as determined by mission needs.
- Briefs, liaisons, and coordinates with a wide-ranging set of Federal, State, local, and private sector partners on a range of cyber issues as determined by mission needs.
- Work with the JRIC and partner agencies to respond, collect and perform forensics analysis of compromised systems.

- Work with the JRIC and the Cal-CSIC incident responders to create relevant and timely cyber products including post incident AARs, vulnerability assessments, executive summaries, and recommended actions to assist California, JRIC and partner entities.
- Investigate, document and report on cybersecurity compromises and emerging trends.
- Provide actionable strategic, tactical, and technical cyber threat information to federal, state, local, tribal, and territorial governmental and private sector partners through weekly, monthly, and ad hoc reports, briefings, and presentations.
- Conduct all-source analysis, digital forensics, and adversary targeting to identify, monitor, assess, and counter the threat posed by foreign cyber actors against US information systems, critical infrastructure, and cyber-related interests.
- Identify an organization's security vulnerabilities and pinpoint indicators of compromise (IOC) such as suspicious IP addresses, URLs, email addresses and attachments, registry keys and filenames.
- Develops cyber indicators to maintain awareness of the status of highly dynamic operating environments and cyber threat actors.
- Attends on-going internal and external training on best practices and sound analytical research and writing skills.
- Attends training on specific subject matters relevant to the assigned subject area.
- Performs duties outlined by NIST Special Publication 800-181 (Workforce Framework for Cybersecurity) for Cyber Defense Analyst.
- Perform other duties as assigned.

Instructions for Submitting Applications

To view the State Active Duty Appointment Application, please click State Active Duty Appointment Application (.pdf). To view California State Guard AHA Form, please click California State Guard AHA Form (.pdf).
Interested applicants must submit a completed and signed State Active-Duty Appointment Application and all required supporting documentation (listed below), to the Director of State Personnel Programs. **Applications missing signatures and required documents will not be considered.**

- **All Applicants:** Documentation of your highest level of civilian education listed on your application. (Legible copy of either diploma, degree, transcripts, Record Brief, RIP).
- **All Applicants:** Are **required** to submit a Resume.
- **All Applicants:** Include any documentation for current flagging actions. SM must include a memo signed by commander indicating circumstances and disposition mitigation.
- **All Applicants:** DMV Printout current within the past six months. California residents may obtain, at cost, a copy of their DMV printout. Unit DMV reports are not accepted.
- **CA Army National Guard (CAARNG) Applicants:** Attach most recent APFT/ACFT (DA Form 705) and MEDPROS IMR**.**
- **CAARNG Applicants:** Are required to submit a Record Brief (ER/ORB) current within the past six months.
- **CAARNG Applicants:** Are required to submit a Soldier Management Record printout (from Retirement Points Accounting System). **(Officer only)**
- **CA Air National Guard (CAANG) Applicants:** Are required to submit Report on Individual Person (RIP), and ARCNet Individual Readiness Detail, current within the past twelve months.

- **CA State Guard (CSG) Applicants:** Complete and submit the CA 3024-1 Member AHA Form. Once appointed, each CSG service member will be required to complete and submit, in its entirety, additional SAD Medical Readiness Standards requirements, not to exceed beyond one year after hire date.
- **CSG Applicants:** CSG Accession Orders and Current Assignment Orders – CSG Applicants only.
- **Deployed Service Members:** Title 10 OCONUS Orders - Currently deployed service members only.

Complete applications and all supporting documents may either be mailed to California Military Department, Director of State Personnel Programs, Attn: NGCA-JSD-SP (Box #27), 10601 Bear Hollow Drive, Rancho Cordova, CA 95670, **Or** e-mailed as **One PDF file** to SP.SADApplication@cmd.ca.gov. Applications mailed, or e-mailed, must be received by the State Personnel office no later than **midnight on Wednesday 8 May 2024.**