

State of California, Military Department
State Active Duty (SAD)
Vacancy Announcement

1 Position Available
(Current SAD Employees Only)

Position Details

Announcement Number: SAD VA 2026-072
Opening Date: 7 August 2026
Closing Date: 20 August 2026
Position Title: Cyber Network Defense (CND) Chief (SAD O-5)
Duty Location: J3-Cyber CND, Sacramento, CA
Selecting Official: Chief of Cyber Operations, Joint-Cyber/Cal-CSIC
Projected Employment Date: TBD

Vacancy Announcement Details

The California Military Department is accepting applications for the State Active-Duty position indicated above. 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 15 November 2024. 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 O-5.** 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 **O-4 through O-6** may apply. Applicants must have a militia affiliation per Para 5-2 of CMD Reg. 600-1. CSG members who have no prior federal militia experience must be a member of the CSG in good standing for a minimum of two years for eligibility for SAD vacancies.
- Knowledge of cyber network defense and vulnerability assessment tools, including open source tools, and their capabilities.
- Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration Protocol, Domain Name System (DNS), and directory services.
- Skills in using network analysis tools to identify vulnerabilities.

- Knowledge of Information Assurance principles related to confidentiality, integrity, availability, authentication, and non-repudiation.
- Knowledge of intrusion detection methodologies and techniques using intrusion detection system tools, applications, and scripts.
- Candidate is required to complete a DOJ/FBI background check.
- Position requires travel up to 50% of the time for periods of up to two weeks per month in an alternate duty location.
- Incumbent compliance with DoD MOS IT requirements to include baseline Operating System and minimum mandatory security certifications for a CNDSP Analyst is preferred.
- ***Must be eligible for EPC/GOEPC Consideration per regulations and board charter.***
- Applicants must maintain good standing with militia component.
- Completion of militia and civilian education requirements commensurate with the grade of the applicant are required.
- Militia assignments appropriate to the grade of the applicant are required.
- Applicants must meet, and maintain, militia component medical and physical fitness standards.
- Appropriate militia uniform with federal or state recognized rank will be worn in accordance with militia regulation.
- Must be able to pass State and Federal background checks (Live Scan), and California Military Department status verification. Continuation of employment is contingent upon maintaining favorable background checks.
- Must possess a valid California driver's license.

Primary Duties and Responsibilities

Supervisory Controls: Chief of Cyber Operations.

- Responsible for providing both strategic and highly technical expertise and advice to the State Chief Information Security Officer, and the California Military Department Chief of Cyber.
- Supervises a team of up to 26, comprised of both technical and administrative staff.
- Responsible to direct, perform, and oversee Cyber Penetration Tests and Vulnerability Assessments; required to have technical expertise and experience to perform these functions directly.
- Responsible for review, impact assessment, and implementation of federal, state, and local directives related to information security.
- Responsible for review and analysis of state policies related to Information Security.
- Reviews departmental requirements related to current computer industry technology, including the practices on data security, integrity, availability, audit compliance, product evaluation, installation, maintenance, and control of information systems software.
- Incumbent frequently manages cross division projects.
- This position includes technical oversight and management of Information Systems computer viral defense, vulnerability mitigation, and network perimeter defense including intrusion detection and prevention systems.

Instructions for Submitting Applications

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/or required documents will not be considered.**

- **All Applicants:** State Active-Duty Appointment Application. To view the State Active Duty Appointment Application, please click [State Active Duty Appointment Application \(.pdf\)](#).
- **All Applicants:** Documentation of your highest level of civilian education listed on your application. (Legible copy of either diploma, degree, transcripts, record brief, RIP, etc.).
- **All Applicants:** Authorization for Release of Information Form. To view Authorization for Release Form, please click [Authorization to Release Information Form \(.pdf\)](#).
- **All Applicants:** Are **required** to submit a Resume.
- **All Applicants:** Unit Verification Memorandum with Unit/BDE Legal clearance (not Security Clearance) letter or email. CAARNG/CAANG verification memos are valid for 6 months from the date of signature. California State Guard applicants will have the memorandum completed by CSG HQ. CSG verification memos are valid for 30 Days from the date of signature. To view Unit Verification Memorandum Template, please click [Unit Verification Memorandum Template \(.pdf\)](#).
- **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:** Are required to submit a Record Brief (ORB) or IPPS-A printout, 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 six months.
- **California State Guard (CSG) Applicants:** CSG Accession Orders and Current Promotion Orders.
- **Deployed Service Members:** Title 10 OCONUS Orders - Currently deployed Service Members only.

Complete applications and all supporting documents may be e-mailed to the California Military Department as **One PDF file** to SP.SADApplication@cmd.ca.gov. Applications must be received by the State Personnel office no later than **midnight on Thursday, 20 August 2026**.

Statement of Qualifications:

A Statement of Qualifications is REQUIRED and must be submitted with your Employment Application.

Applications received without an appropriate Statement of Qualifications based on the instructions below will be rejected for being incomplete and will not be considered. Resumes, cover letters, and other documents will not be considered as a response to the Statement of Qualifications. Please limit your SOQ to a maximum of two (2) pages, single-spaced, no less than twelve-point Arial font.

Candidate must clearly and concisely identify experience in categories listed below and must be in the following order:

- **Leadership and Supervisory Experience.**
- **Collaboration and Conflict-Resolution Skills.**

- **Broad Information Technology Experience.**