

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

### Position Details

Announcement Number: SAD VA 2020-089  
Opening Date: 13 October 2020  
Closing Date: 28 October 2020  
Position Title: Cyber Instructor (SAD E-6)  
Duty Location: JTF-Cyber, Mather, CA  
Selecting Official: Director, JTF-Cyber  
Projected Employment Date: 1 December 2020

### Vacancy Announcement Details

The Military Department is accepting applications for the State Active Duty position indicated above. This vacancy announcement expires **28 October 2020** unless sooner rescinded. 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 w/ Change #1. 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-6.**

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 (Air, Army, CSG) in the grades E-5 through E-7 may apply. Applicants must have a military affiliation per Para 3-2 of CMD Reg. 600-1. Applicants who are not current members of the California Military Department may apply, however, applicants must meet military affiliation requirements at the time of appointment. 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. Non-members of the California Military Department (Air, Army, CSG) must submit a Letter of Intent to meet qualifying military affiliation at the time of appointment along with their application.

- Completion of military (NCO Academy) and civilian education (High School diploma or equivalent) requirements commensurate with the grade of the applicant are required. Attach documentation of your highest level of civilian education.
- Applicant 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) upon hire date. 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.
- Must possess, at minimum, a SECRET clearance, however, a TOP SECRET clearance with Sensitive Compartmented Information eligibility is preferred.

**The following knowledge, skill and abilities will be considered when making the selection but are not all required.**

- Cyber Security knowledge or experience demonstrable through professional certifications or experience in the field.
- Experience instructing large groups on complex topics.
- 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 new and emerging information technology (IT) and cybersecurity technologies.
- Knowledge that technology that can be exploited.
- Knowledge of multiple cognitive domains and tools and methods applicable for learning in each domain.
- Knowledge of virtualization technologies and virtual machine development and maintenance.
- Knowledge of the organization's core business/mission processes.
- Knowledge of emerging security issues, risks, and vulnerabilities.
- Knowledge of learning assessment techniques (rubrics, evaluation plans, tests, quizzes).
- Knowledge of computer based training and e-learning services.
- Knowledge of instructional design and evaluation models (e.g., ADDIE, Smith/Ragan model, Gagne's Events of Instruction, Kirkpatrick's model of evaluation).
- Knowledge of organizational training policies.
- Knowledge of learning levels (i.e., Bloom's Taxonomy of learning).
- Knowledge of Learning Management Systems and their use in managing learning.
- Knowledge of learning styles (e.g., assimilator, auditory, kinesthetic).
- Knowledge of modes of learning (e.g., rote learning, observation).
- Knowledge of organizational training systems.

- Knowledge of media production, communication, and dissemination techniques and methods, including alternative ways to inform via written, oral, and visual media.
- Knowledge of principles and processes for conducting training and education needs assessment.
- Knowledge of relevant concepts, procedures, software, equipment, and technology applications.
- Knowledge of Test & Evaluation processes for learners.
- Knowledge of training and education principles and methods for curriculum design, teaching and instruction for individuals and groups, and the measurement of training and education effects.
- Knowledge of an organization's information classification program and procedures for information compromise.
- Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/training and Research & Development).
- Knowledge of technical delivery capabilities and their limitations.
- Knowledge of cyber competitions as a way of developing skills by providing hands-on experience in simulated, real-world situations.
- Skill in reverse engineering (e.g., hex editing, binary packaging utilities, debugging, and strings analysis) to identify function and ownership of remote tools.
- Skill in reviewing and editing assessment products.
- Skill in technical writing.
- Skill in using tools, techniques, and procedures to remotely exploit and establish persistence on a target.
- Skill in writing about facts and ideas in a clear, convincing, and organized manner.
- Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).
- Skill to remain aware of evolving technical infrastructures.
- Ability to prepare and deliver education and awareness briefings to ensure that systems, network, and data users are aware of and adhere to systems security policies and procedures.
- Ability to answer questions in a clear and concise manner.
- Ability to ask clarifying questions.
- Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.
- Ability to communicate effectively when writing.
- Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.
- Ability to facilitate small group discussions.
- Ability to gauge learner understanding and knowledge level.
- Ability to prepare and present briefings.
- Ability to produce technical documentation.
- Ability to provide effective feedback to students for improving learning.
- Ability to apply principles of adult learning.
- Ability to design valid and reliable assessments.
- Ability to develop clear directions and instructional materials.
- Ability to develop curriculum for use within a virtual environment.
- Ability to operate common network tools (e.g., ping, traceroute, nslookup).
- Ability to tailor curriculum that speaks to the topic at the appropriate level for the target audience.
- Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).

- Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).
- Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.
- Ability to apply critical reading/thinking skills.
- Ability to evaluate information for reliability, validity, and relevance.
- Ability to function in a collaborative environment, seeking continuous consultation with other analysts and experts—both internal and external to the organization—to leverage analytical and technical expertise.
- Ability to tailor technical and planning information to a customer’s level of understanding.
- Ability to think critically.
- Ability to monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.
- Ability to develop or procure curriculum that speaks to the topic at the appropriate level for the target.
- Ability to understand technology, management, and leadership issues related to organization processes and problem solving.
- Ability to understand the basic concepts and issues related to cyber and its organizational impact.
- Ability to conduct training and education needs assessment.

### Primary Duties and Responsibilities

Supervised by the California Office of Emergency Services, Cyber Security Integration Center Support Branch Chief, or designee. The Support Branch Chief, or designee, will provide day-to-day supervision, assignment of work schedule and validation of hours worked by the employee Provides leadership, mentorship, technical guidance and support to cadets in educational, vocational, physical training, job placement, community service and leadership programs.

#### **The following tasks may be assigned, depending on the needs of the department:**

- Provide leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
- Conduct training of personnel within pertinent subject domain. Develop, plan, coordinate, deliver and/or evaluate training courses, methods, and techniques as appropriate.
- Develop and conduct training or education of personnel within cyber domain.
- Conduct interactive training exercises to create an effective learning environment.
- Develop new or identify existing awareness and training materials that are appropriate for intended audiences.
- Evaluate the effectiveness and comprehensiveness of existing training programs.
- Review training documentation (e.g., Course Content Documents [CCD], lesson plans, student texts, examinations, and Schedules of Instruction [SOI], and course descriptions).
- Support the design and execution of exercise scenarios.
- Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce.
- Develop or assist in the development of computer based training modules or classes, development of course assignments, course evaluations, and of grading and proficiency standards.
- Assist in the development of individual/collective development, training, and/or remediation plans.
- Develop or assist in the development of learning objectives and goals, on-the-job training materials or programs, and written tests for measuring and assessing learner proficiency.

- Conduct learning needs assessments and identify requirements.
- Develop or assist in the development of training policies and protocols for cyber training.
- Develop the goals and objectives for cyber curriculum.
- Present technical information to technical and nontechnical audiences.
- Present data in creative formats.
- Write and publish after action reviews.
- Deliver training courses tailored to the audience and physical/virtual environments.
- Apply concepts, procedures, software, equipment, and/or technology applications to students.
- Design training curriculum and course content based on requirements.
- Participate in development of training curriculum and course content.
- Ensure that training meets the goals and objectives for cybersecurity training, education, or awareness.
- Plan and coordinate the delivery of classroom techniques and formats (e.g., lectures, demonstrations, interactive exercises, and multimedia presentations) for the most effective learning environment.
- Plan non-classroom educational techniques and formats (e.g., video courses, mentoring, web-based courses).
- Recommend revisions to curriculum and course content based on feedback from previous training sessions.
- Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media).
- Develop or assist with the development of privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations.
- Performs other duties as assigned.

### Instructions for Submitting Applications

To request a State Active Duty Appointment Application or CSG AHA forms, please contact State Personnel Programs by email at [ng.ca.caarng.mbx.sad-application@mail.mil](mailto:ng.ca.caarng.mbx.sad-application@mail.mil) for assistance.

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, or transcripts).
- **Readiness:** Include any documentation for current flagging actions. SM must include memo signed by commander indicating circumstances and disposition mitigation.
- **CA Army National Guard (CAARNG) Applicants:** APFT (DA Form 705) and MEDPROS IMR, current within the past twelve months. **(Due to the CA NG inability to conduct APFT qualification during the current COVID - 19 Restrictions, the 12 month APFT (DA Form 705) requirement has been extended to: Current within the past 18 months).**
- **CA Air National Guard (CA ANG) Applicants:** ARCNet Individual Readiness Detail, current within the past twelve months. **(Due to the CA NG inability to conduct APFT qualification during the current COVID - 19 Restrictions, the 12 month ARCNET requirement has been extended to: Current within the past 18 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.
- **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.
- **CSG Applicants:** CSG 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 Joint Force Headquarters, Director of State Personnel Programs, Attn: NGCA-JSD-SP (Box #27), 9800 Goethe Road, Sacramento, CA 95827, **Or** e-mailed as **One PDF file** to [ng.ca.caarng.mbx.sad-application@mail.mil](mailto:ng.ca.caarng.mbx.sad-application@mail.mil). Applications mailed, or e-mailed, must be received by the State Personnel office no later than the **close of business on Wednesday, 28 October 2020**.