

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

### Position Details

Announcement Number: SAD VA 2020-092  
Opening Date: 13 October 2020  
Closing Date: 28 October 2020  
Position Title: All-Source Analyst (SAD CW2)  
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 This vacancy announcement expires **28 October 2020** unless sooner rescinded.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 CW2.**

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 WOC through CW3 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.**

- 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 human-computer interaction principles.
- Knowledge of network traffic analysis methods.
- Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless).
- Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).
- Knowledge of cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
- Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).
- Knowledge of website types, administration, functions, and content management system (CMS).
- Knowledge of analytical constructs and their use in assessing the operational environment
- Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).
- Knowledge of classification and control markings standards, policies and procedures.
- Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).
- Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.).
- Knowledge of current computer-based intrusion sets.
- Knowledge of cyber intelligence/information collection capabilities and repositories.
- Knowledge of cyber laws and their effect on Cyber planning.
- Knowledge of encryption algorithms and cyber capabilities/tools (e.g., SSL, PGP).

- Knowledge of evolving/emerging communications technologies.
- Knowledge of fundamental cyber operations concepts, terminology/lexicon (i.e., environment preparation, cyber-attack, cyber defense), principles, capabilities, limitations, and effects.
- Knowledge of general Supervisory control and data acquisition (SCADA) system components.
- Knowledge of host-based security products and how those products affect exploitation and reduce vulnerability.
- Knowledge of how Internet applications work (SMTP email, web-based email, chat clients, VOIP).
- Knowledge of how modern digital and telephony networks impact cyber operations.
- Knowledge of how modern wireless communications systems impact cyber operations.
- Knowledge of how to extract, analyze, and use metadata.
- Knowledge of intelligence confidence levels.
- Knowledge of intelligence disciplines.
- Knowledge of intelligence preparation of the environment and similar processes.
- Knowledge of intelligence support to planning, execution, and assessment.
- Knowledge of internal and external partner cyber operations capabilities and tools.
- Knowledge of internal tactics to anticipate and/or emulate threat capabilities and actions.
- Knowledge of Internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering).
- Knowledge of malware.
- Knowledge of organization or partner exploitation of digital networks.
- Knowledge of organizational hierarchy and cyber decision-making processes.
- Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.
- Knowledge of specific target identifiers, and their usage.
- Knowledge of target development (i.e., concepts, roles, responsibilities, products, etc.).
- Knowledge of target vetting and validation procedures.
- Knowledge of targeting cycles.
- Knowledge of telecommunications fundamentals.
- Knowledge of the basic structure, architecture, and design of modern communication networks.
- Knowledge of the basics of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).
- Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.
- Knowledge of the intelligence frameworks, processes, and related systems.
- Knowledge of the structure and intent of organization specific plans, guidance and authorizations.
- Knowledge of the ways in which targets or threats use the Internet.
- Knowledge of threat and/or target systems.
- Knowledge of virtualization products (VMware, Virtual PC).
- Knowledge of what constitutes a “threat” to a network.
- Knowledge of wireless technologies (e.g., cellular, satellite, GSM) to include the basic structure, architecture, and design of modern wireless communications systems.
- Skill in assessing and/or estimating effects generated during and after cyber operations.
- Skill in conducting non-attributable research.

- Skill in defining and characterizing all pertinent aspects of the operational environment.
- Skill in developing or recommending analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.
- Skill in evaluating information for reliability, validity, and relevance.
- Skill in identifying alternative analytical interpretations to minimize unanticipated outcomes.
- Skill in identifying cyber threats which may jeopardize organization and/or partner interests.
- Skill in preparing and presenting briefings.
- Skill in providing analysis to aid writing phased after action reports.
- Skill in providing understanding of target or threat systems through the identification and link analysis of physical, functional, or behavioral relationships.
- Skill in tailoring analysis to the necessary levels (e.g., classification and organizational).
- Skill in using Boolean operators to construct simple and complex queries.
- Skill in using multiple analytic tools, databases, and techniques (e.g., Analyst's Notebook, A-Space, Anchory, M3, divergent/convergent thinking, link charts, matrices, etc.).
- Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches.
- Skill in utilizing feedback to improve processes, products, and services.
- Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).
- Skill in writing, reviewing and editing cyber-related Intelligence/assessment products from multiple sources.
- Skill to analyze and assess internal and external partner cyber operations capabilities and tools.
- Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.
- Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.
- Ability to develop or recommend analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.
- Ability to evaluate, analyze, and synthesize large quantities of data (which may be fragmented and contradictory) into high quality, fused targeting/intelligence products.
- Ability to clearly articulate intelligence requirements into well-formulated research questions and data tracking variables for inquiry tracking purposes.
- Ability to effectively collaborate via virtual teams.
- Ability to evaluate information for reliability, validity, and relevance.
- Ability to exercise judgment when policies are not well-defined.
- Ability to focus research efforts to meet the customer's decision-making needs.
- Ability to function effectively in a dynamic, fast-paced environment.
- 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 identify intelligence gaps.
- Ability to recognize and mitigate cognitive biases which may affect analysis.
- Ability to recognize and mitigate deception in reporting and analysis.
- Ability to think critically.

- Ability to think like threat actors.
- Ability to understand objectives and effects.
- Ability to utilize multiple intelligence sources across all intelligence disciplines.

### Primary Duties and Responsibilities

Supervised by the California Office of Emergency Services, Cyber Security Integration Center Intelligence Branch Chief, or designee. The Intelligence 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:**

- Analyze threat information. Synthesize and place intelligence information in context; draw insights about the possible implications.
- Analyze data/information to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.
- Performing highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
- Answer requests for information.
- Provide expertise to course of action development.
- Provide subject matter expertise to the development of a common operational picture.
- Maintain a common intelligence picture.
- Provide subject matter expertise to the development of cyber operations specific indicators.
- Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.
- Assist in the identification of intelligence collection shortfalls.
- Brief threat and/or target current situations.
- Collaborate with intelligence analysts/targeting organizations involved in related areas.
- Conduct in-depth research and analysis.
- Conduct nodal analysis.
- Maintain awareness of internal and external cyber organization structures, strengths, and employments of staffing and technology.
- Develop information requirements necessary for answering priority information requests.
- Engage customers to understand customers' intelligence needs and wants.
- Evaluate threat decision-making processes.
- Identify threat vulnerabilities.
- Identify threats to Blue Force vulnerabilities.
- Generate requests for information.
- Identify threat tactics, and methodologies.
- Identify and evaluate threat critical capabilities, requirements, and vulnerabilities.
- Identify and submit intelligence requirements for the purposes of designating priority information requirements.
- Identify intelligence gaps and shortfalls.

- Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets.
- Monitor and report on validated threat activities.
- Monitor open source websites for hostile content directed towards organizational or partner interests.
- Monitor operational environment and report on adversarial activities which fulfill leadership's priority information requirements.
- Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).
- Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate.
- Provide subject matter expertise to website characterizations.
- Provide analyses and support for effectiveness assessment.
- Provide current intelligence support to critical internal/external stakeholders as appropriate.
- Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations.
- Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations.
- Provide input and assist in post-action effectiveness assessments.
- Provide input and assist in the development of plans and guidance.
- Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations.
- Provide target recommendations which meet leadership objectives.
- Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities.
- Report intelligence-derived significant network events and intrusions.
- Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.
- 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.**