

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

Position Details

Announcement Number: SAD VA 2020-088
Opening Date: 13 October 2020
Closing Date: 28 October 2020
Position Title: Vulnerability Assessment Analyst (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 This vacancy announcement expires **28 October 2020** unless sooner rescinded.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.

- 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 application vulnerabilities.
- Knowledge of cryptography and cryptographic key management concepts
- Knowledge of data backup and recovery.
- Knowledge of host/network access control mechanisms (e.g., access control list, capabilities lists).
- Knowledge of cybersecurity and privacy principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
- Knowledge of network access, identity, and access management (e.g., public key infrastructure, OAuth, OpenID, SAML, SPML).
- Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).
- Knowledge of programming language structures and logic.
- Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
- Knowledge of systems diagnostic tools and fault identification techniques.
- Knowledge of what constitutes a network attack and a network attack's relationship to both threats and vulnerabilities.
- Knowledge of interpreted and compiled computer languages.
- Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution attacks).

- Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).
- Knowledge of system administration, network, and operating system hardening techniques.
- Knowledge of cyber-attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
- Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).
- Knowledge of ethical hacking principles and techniques.
- Knowledge of data backup and restoration concepts.
- Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.
- Knowledge of infrastructure supporting information technology (IT) for safety, performance, and reliability.
- Knowledge of an organization's information classification program and procedures for information compromise.
- Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).
- Knowledge of cryptology.
- Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
- Knowledge of penetration testing principles, tools, and techniques.
- Knowledge of an organization's threat environment.
- Knowledge of Application Security Risks (e.g. Open Web Application Security Project Top 10 list)
- Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.
- Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).
- Skill in mimicking threat behaviors.
- Skill in the use of penetration testing tools and techniques.
- Skill in the use of social engineering techniques. (e.g., phishing, baiting, tailgating, etc.).
- Skill in using network analysis tools to identify vulnerabilities. (e.g., fuzzing, nmap, etc.).
- Skill in reviewing logs to identify evidence of past intrusions.
- Skill in conducting application vulnerability assessments.
- Skill in performing impact/risk assessments.
- Skill to develop insights about the context of an organization's threat environment
- Skill to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).
- Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.
- Ability to apply programming language structures (e.g., source code review) and logic.
- Ability to share meaningful insights about the context of an organization's threat environment that improve its risk management posture.
- Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).

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.

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

- Identify, analyze, and mitigate threats to internal information technology (IT) systems and/or networks.
- Conduct assessments of threats and vulnerabilities; determine deviations from acceptable configurations, enterprise or local policy; assess the level of risk; and develop and/or recommend appropriate mitigation countermeasures in operational and nonoperational situations.
- Perform assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measure effectiveness of defense-in-depth architecture against known vulnerabilities.
- Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational
- Conduct and/or support authorized penetration testing on enterprise network assets.
- Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions.
- Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.
- Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.
- Conduct required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews).
- Perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications).
- Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes).
- 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 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. 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.**