State of California, Military Department

State Active Duty (SAD)

Vacancy Announcement

Multiple Position's Available

(TEMP Position)

Position Details

Announcement Number:	SAD VA 2021-072
Opening Date:	29 September 2021
Closing Date:	14 October 2021
Position Title:	Cyber Analyst I (SAD E-5)
Duty Location:	Okinawa Armory, Sacramento, CA
Selecting Official:	Chief Cyber Network Defense
Projected Employment Date:	15 November 2021

Vacancy Announcement Details

The Military Department is accepting applications for the State Active Duty position indicated above. This vacancy announcement expires **14 October 2021** unless sooner rescinded.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, 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-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 (Air, Army, CSG) in the grades **E-4 through E-6** 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.

- **This is a 12 month temporary position.**
- Completion of military and civilian education 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.
- 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.)**
- Must have a flexible schedule. Duty hours are depended upon customer driven work schedules and may include extended hours, alternative shifts, and weekends.
- Candidate is required to supplement 24/7 operational support for assigned cyber incident response missions impacting State of California, local municipality, and regional critical infrastructure information assets as required by official Mission Request Tasking (MRT) assignments from the Governor's Office Of Emergency Services (CalOES), or California Cybersecurity Integration Center (Cal-CSIC).
- 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, Domain Name System (DNS), and directory services.
- Skill in using network analysis tools to identify vulnerabilities.
- Knowledge of Information Assurance principles related to confidentiality, integrity, availability, authentication, non-repudiation.
- Knowledge of intrusion detection methodologies and techniques using instruction detection system tools, applications, and scripts.
- Minimum valid Secret security clearance upon hire. Candidate acknowledges the requirement to submit for a Top-Secret clearance with Sensitive Compartmented Information (TS/SCI) access depending on assignment.
- Position requires travel up to 50% of the time for periods of up to two weeks per month in an alternate location.
- On-site portions of the Independent Security Assessment (ISA) program cannot be conducted via remote / work-from-home accommodations.
- Incumbent must comply with requirements of DoD 8570.1M which include both an approved baseline Operating System and minimum mandatory security certifications for a CNDSP Analyst; see http://iase.disa.mil/iawip/Pages/iabasline.aspx for additional information.
- 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 California driver's license. **Attach a current copy, within the past six months, of your Department of Motor Vehicle's printout.**

Primary Duties and Responsibilities

CND Team Chief (SAD)

State Computer Network Defense Operations Manager (ITM-II)

- Perform full scope vulnerability assessments, analysis and network security assessments to CMD units, other National Guard states (through EMAC process), State Agencies, and Critical Infrastructure Partners.
- Examine network topologies to understand data flows through the network.
- Characterize and analyze network traffic to identify anomalous activity and potential threats to network assets.
- Document risk finding and countermeasure recommendations.
- Prepare, maintain, and use Cyber Network Defense tools to detect potential configuration and security risks.
- Protect Network Information Assets.
- Conduct tests of information Assurance safeguards in accordance with the scope of authorized Tactics, Techniques, and Procurers (TTPs).
- Prepare risk and analysis reports.
- Provide hands-on security support.
- Interpret network configurations against established baseline, regulatory, and technical guidelines and document findings.
- Analyze network traffic collected during customer engagements for indications of compromise.
- Detect signs of attempted network or system intrusion.
- Develop best business practice-based incident response steps.
- Upon direction, implement approved incident response plan.
- Document incident response findings.
- Perform ISA operations during established entity operational windows, avoiding network / host critical operational hours that may include varying shifts, spanning extended hours (12-hour days), including out-of-business hour periods Preserve incident documentation, event logs, and configurations using forensic and law enforcement standards.
- Assist with network hardening and reconfigurations.
- Participate in post-mortem analysis review of incident.
- Provide regulatory, guideline, policy, and configuration analysis for best practice implementations.
- Support training and mentorship to supported CMD Units, partners, and agencies with regards to best practice security configuration and implementations.
- Prepare technical overview briefings for Department of Defense Support Activities and External Customers.
- Brief CND Manager on current projects, efforts, and findings.
- 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 SP.SADApplication@cmd.ca.gov 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: Are required to submit documentation of COVID-19 vaccination.**
- **All Applicants:** Documentation of your highest level of civilian education listed on your application. (Legible copy of either diploma, degree, or transcripts).
- **All Applicants:** Are required to submit the attached Statement of Qualification's (SOQ) (please see below), and are strongly encouraged to submit a current Resume.

- **Readiness:** Include any documentation for current flagging actions. SM must include memo signed by commander indicating circumstances and disposition mitigation.
- **All CAARNG Applicants**: Are required to submit Enlisted Record Brief (ERB).
- **CA Army National Guard (CAARNG) Applicants:** Attach 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 31 March 2022 and must not be dated any later than 31 March 2019. Army Directive 2020-006 (Army Combat Fitness Test) allows Soldiers to continue to take and record an APFT to overcome a flag.**
- **CA Air National Guard (CA ANG) 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.
- **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 and DD 214 (if less than two years CSG) – 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 SP.SADApplication@cmd.ca.gov. Applications mailed, or e-mailed, must be received by the State Personnel office no later than the **close of business on Thursday, 14 October 2021.**

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.

1. Describe your background, experience, education, and/or training regarding the conduct of information system vulnerability assessment scanning.
2. Describe your background, experience, education and/or training regarding the configuration, troubleshooting, and administration of windows/Linux operating systems and networking infrastructure devices within an enterprise environment.
3. Describe your background, experience, education and/or training regarding the application of cybersecurity frameworks controls (e.g. NIST, ISO, PCI, Fed Ramp).
4. Describe examples of technical and non-technical information technology report writing experience. Please include the intended audience.
5. Describe your background, experience, education, and/or training regarding the capture and analysis of information technology network traffic using industry common tools (e.g., Wireshark, t-shark, Solar Winds, or other similar technologies).
6. Describe your prior experience developing and presenting information technology technical presentations to peers, superiors, and executives