State of California, Military Department

State Active Duty (SAD)

Vacancy Announcement

1 Position Available

Position Details

Announcement Number:	SAD VA 2025-025
Opening Date:	28 February 2025
Closing Date:	14 March 2025
Position Title:	Senior Cyber Analyst II (SAD E-6/CW3/O-3)
Duty Location:	J3/Cyber Network Defense, Sacramento
Selecting Official:	Cyber Network Defense Chief
Projected Employment Date:	15 April 2025

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 (CSG) pay grade, not to exceed E-6/CW3/O-3.** 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 Employee Assistance Programs, Group Legal Services, Long-Term Disability Insurance, Long-Term Care Insurance, Retirement Annuity, Savings Plus, 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 **E-2 through E-8/WO1 through CW4/O-1 through O-6** may apply. Applicants must have a military affiliation per Para 5-2 of CMD Reg. 600-1. 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.
- Duty location: California Military Department (CMD), Cyber Network Defense (CND)8450 Okinawa St, Sacramento, CA 95828.
- 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.)

- Be fully compliant with current and ongoing changes to California Military Department (CMD) hiring/retention requirements regarding vaccination status, physical and dental readiness, and adverse personnel action status.
- On-site portions of the Independent Security Assessment (ISA) and Local Educational Agency (LEA) programs may need to be supported with on-site attendance. Candidate must comply with all State of California, CMD, and supported entity on-site health and safety requirements.
- Routine local travel is required 50% monthly; State-wide/Out-of-State travel up to 20% monthly.
- Deploying, monitoring, and interpreting the results obtained from network protocol analyzers.
- Creation, selection, deployment, and management of phishing campaigns designed to elicit user response and credential surrender.
- Implementation of Defense-In-Depth principles within network security architectures.
- Deployment, troubleshooting and result analysis using the Security Content Automation Protocol (SCAP) tools within enterprise networked environments.
- Troubleshooting network mapping and operating system (OS) fingerprinting activities within enterprise environments.
- Common networking tools including but not limited to ping, traceroute, nslookup,Whois, Netstat.
- Network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.
- Network traffic flows (e.g., Transmission Control Protocol (TCP), Internet Protocol (IP), and the Open System Interconnection Model (OSI)).
- Cyber Network Defense policies, procedures, and regulations (State and Federal).
- Incumbent must be able to effectively communicate with team members, external partner agencies, and supervisors.
- Prior technical experience performing research, guidance, and resource support in the areas of analysis, characterization, and technical research related to anomalous activity and potential threats to network resources in direct support to Cyber Analyst team members.
- Incumbent must be able to effectively provide briefings and other educational interactions with CMD staff, supported entities, and other partner activities.
- An active US Government Security Clearance at the Secret level is required for all assigned team members in order to attend all Cal-CSIC (DHS-Cyber) Classified Tactics, Techniques, and Procedures briefings.
- Depending on internal team role assignment, incumbent may be required to acquire and maintain an active US Government Security at the Top Secret (with SCI Caveat) level to participate in intelligence community information exchange, including access to current threat actor Tactics, Techniques, and Procedures from US Cyber Command, National Guard Bureau Cyber and FBI Cyber as part of an ongoing cyber. hunt and incident response activities.
- Incumbent will be notified if assigned to said role.
- Successful candidate must successfully progress in all assigned educational requirements as a condition continued assignment.
- Individual must comply with the requirements of the DoD Cyber Workforce, Information Assurance (IA) Workforce Qualification Program which includes both an approved baseline Operating System (OS) and minimum mandatory security certifications for at the CND Analyst level; see https://public.cyber.mil/cw/cwmp/summary for additional information.

- Successful completion/certification of these requirements every 6 months is sufficient for continued position assignment consideration.
- Candidate acknowledges if they are unable to successfully certify or maintain certification, then the candidate acknowledges they must be reassigned to a new role. Depending on availability and grade, this may preclude further assigned within the CND or may be grounds separation.
- Ongoing Educational Requirements (Role Specific): IT positions are ever evolving, highly technical, and address continuously evolving technologies. CND provides role-specific, no-cost, educational training courses to members to address these requirements.
- Effective time management and course completion of assigned role-specific training is an evaluated criteria for continued position assignment consideration.
- 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 state driver's license.

Primary Duties and Responsibilities

Rated by Penetration Tester.
Senior Rated by Chief, Cyber Network Defense.

- Primary point of contact during Risk Analysis Phase of assessments.
- Perform full scope Vulnerability and network security assessments and analysis.
- Analyze network traffic collected during customer engagements for indications of compromise.
- Analyst II job includes protecting our organization's digital assets by identifying and validating potential security weaknesses.
- Will actively contribute to the implementation of security countermeasures on CND networks to ensure the highest level of security.
- Document risk finding and countermeasure recommendations.
- Provide regulatory, guideline, policy, and configuration analysis for best practice implementations.
- Prepare technical overview briefings. Briefs Cyber Network Defense Team Manager on current projects, efforts, and findings.
- Conduct cybersecurity defensive analysis on state agency networks in support of California Department of Technology, Office of Information Security, Independent Security Assessments (ISA) in support of Section 11549.3 of State of California Government Code.
- Conduct cybersecurity defensive analysis on Local Educational Agency (LEA) networks in support of Section 11549.3 of State of California Government Code.
- Supervise the conduct of Risk Analysis (RA) operations in support of ISA and LEA programs.

- Supervise and conduct ISA/LEA operations during agreed upon entity operational windows that may require varying shifts, spanning extended hours (12-hour days), including out-of-business hour periods.
- Provide direction, mentorship, guidance, and team leader supervision to subordinate CND Analyst I and other assigned augmentation personnel.
- Provide Tier-II analysis, characterization, and technical research related to anomalous activity and potential threats to network resources.
- Candidate is part of a mobile support delivery team that works onsite at the supported entity site(s).
- Perform equipment inventory, validate readiness, and ensure sensitive data sanitization prior to mission deployment, and secure/protect assigned and entity provided equipment.
- Prepare and provide highly technical briefings in support of ISA and LEA programs as required to various senior executive level mission partners to include Agency CIO, CISO and senior IT staff.
- Support training and mentorship with regards to best practice security configuration and implementations.
- Perform vulnerability analysis troubleshooting included but not limited to asset performance impact mitigation, troubleshooting clients and asset scans.
- Perform and monitor on-site, full scope of vulnerability assessment analysis of supported entity IT assets using industry certified applications, techniques, and procedures. Document risk findings and countermeasure recommendations in briefings, reports, and other program deliverables in support of ISA/LEA programs, and IR missions.
- Interpret network configurations against established baseline, regulatory, and technical guidelines and document findings.
- Analyze network traffic collected during customer engagements for indications of compromise.
- Assist team and supported entities with network hardening and reconfigurations.
- Working knowledge of network security and related concepts.
- Review highly technical network topologies for compliance with Defense-in-Depth considerations.
- Prepare technical overview briefings for Senior Joint staff, Directors, Staff elements and cyber defense teams.
- Brief CND management team on current project status, efforts, and findings.
- Provide technical advice and feedback on data collection and processing tactics, techniques, and procedures.
- Design, develop, build, and maintain tools and systems for team use.
- Adherence to all Federal Intelligence Community (IC), Department of Defense, State of California Government Code Section 6250, CMD, and Entity specified protection of information of supported entities.
- Upon receipt of a Mission Request Tasking (MRT) from CalOES/Cal-CSIC, provide network defensive analysis support in response to an approved Emergency Management Assistance Compact (EMAC) to State of California supported government partners (i.e. other states).
- Upon direction of a validated MRT/EMAC tasking, conduct network cyber hunt and Incident Response (IR) actions in support of state networks.
- Preserve incident documentation, event logs, and configurations using forensic and law enforcement standards for artifacts collected/generated in direct support of validated MRT/EMAC tasking.
- Participate in post-mortem analysis review of validated MRT/EMAC tasking cyber incidents to determine TTPs and methods of compromise.

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 letter or email. California State Guard (CSG) applicants will have the memorandum completed by CSG HQ. 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 (ERB/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 Friday, 14 March 2024.**