State of California, Military Department

State Active Duty (SAD)

Vacancy Announcement

Multiple Positions Available (TEMP)

Position Details

Announcement Number:	SAD VA 2026-038
Opening Date:	27 April 2026
Closing Date:	10 May 2026
Position Title:	Cyber Defense Forensics Analyst (SAD E-8/CW3/O-3)
Duty Location:	JTF Cyber/Cal-CSIC, Mather
Selecting Official:	OIC Knowledge Manager, JTF Cyber-Cal-CSIC
Projected Employment Date:	10 June 2026

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. **This position is not to exceed 30 June 2026.** 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-8/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 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 (Army, Air, CSG) in the grades **E-1 through E-9 or WO1 through CW4 or O-1 through O-4** may apply. Applicants must have a militia affiliation per Para 5-2 of CMD Reg. 600-1. CSG members who have no prior federal militia experience must be a member of the CSG in good standing for a minimum of two years for eligibility for SAD vacancies.
- Analysts must have at least one (1) year of experience in cyber security/information assurance, and be able to research, process, create, and brief actionable reports using the information gathered.
- Analysts must be able to utilize critical thinking skills to apply gathered information and intelligence to California specific targets, information requirements, and areas of responsibility.
- 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 and 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

The incumbent of this position will be supervised by the Cyber Operations Senior Incident Responder.

- Collects, processes, preserves, analyzes, and presents computer-related evidence in support of cyber incident response, compromise assessments, threat hunting, network vulnerability mitigation, criminal, and/or law enforcement investigations.
- Analyzes digital evidence and investigates computer security incidents to derive useful information in support of the Cal-CSICs mission statement, the Cyber Operations Branch and the Cyber Threat Intel Branch objectives.
- Ensure chain of custody procedures are followed for all digital media and forensics evidence acquired in accordance with the Federal Rules of Evidence.
- Preserve evidence integrity according to standard operating procedures and national standards.
- Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.
- Utilize deployable and remote forensics toolkits to support operations and mission requirements as necessary.
- Prepare digital media and forensics evidence for imaging and processing by ensuring data integrity techniques in accordance with standard operating procedures.
- Create a forensically sound duplicate of the evidence that ensures the original evidence is not unintentionally modified for data recovery and analysis processes.
- Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.
- Review forensic images and other data sources for recovery of potentially relevant information.
- Perform static, dynamic, media, and file systems analysis.
- Provide technical summary of these findings in accordance with established reporting procedures and style guides.
- Write forensics reports, timelines, analysis reports, and white papers on incident findings to appropriate colleagues, supervisors, communities and requesting organizations.
- Serve as a Cal-CSIC cyber operations team member and a forensics liaison to partner organizations to assist with cyber response activities impacting the state of CA, local, tribal and territorial governments.
- Serves as a point of contact for subject matter material for the Cal-CSIC.
- Ensures appropriate relationships are made at the Federal, State, and local levels for information sharing and coordination activities.
- Works to advance joint, analytical and collaborative opportunities with new and existing Cal-CSIC partners.
- Briefs on cyber incident response & forensics activities as determined by mission needs. Briefs, liaisons, and coordinates with a wide-ranging set of Federal, State, local, and private sector partners on a range of cyber issues as determined by mission needs.

- Works with Cal-CSIC responders and analysts to create relevant and timely cyber forensics products including forensics timelines, post incident reporting, cyber kill chain associations, MITRE ATT&CK mappings, executive summaries, and recommended actions.
- Attend on-going internal and external training on best practices and sound analytical research and writing skills.
- Attends training on specific subject matters relevant to the assigned subject area.
- Perform duties outlined by NIST Special Publication 800-181 (Workforce Framework for Cybersecurity) for Cyber Defense Forensics Analyst.
- Perform other duties as assigned or required to include research, written analysis, cyber incident response, and cyber defense analysis work.
- Conduct Cybersecurity Assessments (CSA) and targeted advisory engagements for State, Local, Tribal, and Territorial entities to identify cybersecurity risks and provide actionable mitigation recommendations.
- Perform technical validation activities including vulnerability scanning, network mapping, configuration review, and security control assessments across enterprise, cloud, and hybrid environments.
- Review identity and access management, system hardening, patch management, logging, and monitoring practices to evaluate organizational cyber hygiene and defensive readiness.

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. A**pplications 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 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 Sunday, 10 May 2026.**