State of California, Military Department

State Active Duty (SAD)

Vacancy Announcement

1 Position Available

Position Details

Announcement Number:	SAD VA 2020-090
Opening Date:	13 October 2020
Closing Date:	28 October 2020
Position Title:	Cyber Operator (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 This vacancy announcement expires **28 October 2020** unless sooner rescinded.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 data backup and recovery.
- Knowledge of low-level computer languages (e.g., assembly languages).
- 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 collection management processes, capabilities, and limitations.
- Knowledge of system administration concepts for operating systems such as but not limited to Unix/Linux, IOS, Android, and Windows operating systems.
- Knowledge of auditing and logging procedures (including server-based logging).
- Knowledge of programming concepts (e.g., levels, structures, compiled vs. interpreted languages).
- Knowledge of basic software applications (e.g., data storage and backup, database applications) and the types of vulnerabilities that have been found in those applications.
- Knowledge of wireless applications vulnerabilities.
- Knowledge of client organizations, including information needs, objectives, structure, capabilities, etc.
- Knowledge of cryptologic capabilities, limitations, and contributions to cyber operations.
- Knowledge of current software and methodologies for active defense and system hardening.
- Knowledge of database theory.
- Knowledge of de-confliction reporting to include external organization interaction.
- Knowledge of encryption algorithms and tools for wireless local area networks (WLANs).
- Knowledge of encryption algorithms and cyber capabilities/tools (e.g., SSL, PGP).

- Knowledge of enterprise-wide information management.
- Knowledge of evasion strategies and techniques.
- Knowledge of forensic implications of operating system structure and operations.
- Knowledge of mobile cellular communications architecture (e.g., LTE, CDMA, GSM/EDGE and UMTS/HSPA).
- Knowledge of host-based security products and how those products affect exploitation and reduce vulnerability.
- Knowledge of implementing UNIX and Windows systems that provide radius authentication and logging, DNS, mail, web service, FTP server, DHCP, firewall, and SNMP.
- Knowledge of internal and external partner reporting.
- Knowledge of methods and techniques used to detect various exploitation activities.
- Knowledge of network administration.
- Knowledge of network construction and topology.
- Knowledge of malware.
- Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.
- Knowledge of satellite-based communication systems.
- Knowledge of security hardware and software options, including the network artifacts they induce and their effects on exploitation.
- Knowledge of security implications of software configurations.
- Knowledge of structure, approach, and strategy of exploitation tools (e.g., sniffers, key loggers) and techniques (e.g., gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network).
- Knowledge of the basic structure, architecture, and design of modern communication networks.
- 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 fundamentals of digital forensics to extract actionable intelligence.
- Knowledge of Unix/Linux and Windows operating systems structures and internals (e.g., process management, directory structure, installed applications).
- Knowledge of virtual machine technologies.
- Skill in processing collected data for follow-on analysis.
- Skill in providing real-time, actionable geolocation information utilizing target infrastructures.
- Skill in reading, interpreting, writing, modifying, and executing simple scripts (e.g., PERL, VBS) on Windows and Unix systems (e.g., those that perform tasks like parsing large data files, automating manual tasks, and fetching/processing remote data).
- Skill in relevant programming languages (e.g., C++, Python, etc.).
- Skill in remote command line and Graphic User Interface (GUI) tool usage.
- Skill in reverse engineering (e.g., hex editing, binary packaging utilities, debugging, and strings analysis) to identify function and ownership of remote tools.
- Skill in server administration.
- Skill in survey, collection, and analysis of wireless LAN metadata.
- Skill in technical writing.
- Skill in testing and evaluating tools for implementation.

- Skill in using tools, techniques, and procedures to remotely exploit and establish persistence on a target.
- Skill in using various open source data collection tools (online trade, DNS, mail, etc.).
- Skill in verifying the integrity of all files. (e.g., checksums, Exclusive OR, secure hashes, check constraints, etc.).
- Skill in wireless network target analysis, templating, and geolocation.
- Skill to analyze and assess internal and external partner reporting.
- Ability to interpret and translate customer requirements into operational action.
- Ability to monitor system operations and react to events in response to triggers and/or observation of trends or unusual activity.
- Ability to perform network collection tactics, techniques, and procedures to include decryption capabilities/tools.
- Ability to perform wireless collection procedures to include decryption capabilities/tools.

Primary Duties and Responsibilities

Supervised by the California Office of Emergency Services, Cyber Security Integration Center Incident Response Branch Chief, or designee. The Incident Response Branch Chief, or designee, will provide day-to-day supervision, assignment of work schedule and validation of hours worked by the employee. Provide specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

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

- Perform activities to gather evidence on criminal or foreign intelligence entities to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.
- Conducts collection, processing, and/or geolocation of systems to exploit, locate, and/or track targets of interest. Performs network navigation and tactical forensic analysis.
- Demonstrable skill or experience in providing specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
- Analyze internal operational architecture, tools, and procedures for ways to improve performance.
- Analyze target operational architecture for ways to gain access.
- Collaborate with development organizations to create and deploy the tools needed to achieve objectives.
- Conduct access enabling of wireless computer and digital networks.
- Conduct collection and processing of wireless computer and digital networks.
- Conduct exploitation of wireless computer and digital networks.
- Conduct network scouting and vulnerability analyses of systems within a network.
- Conduct on-net activities to control and exfiltrate data from deployed technologies.
- Conduct on-net and off-net activities to control, and exfiltrate data from deployed, automated technologies.
- Conduct open source data collection via various online tools.
- Conduct survey of computer and digital networks.
- Deploy tools to a target and utilize them once deployed (e.g., backdoors, sniffers).
- Detect exploits against targeted networks and hosts and react accordingly.
- Develop new techniques for gaining and keeping access to target systems.
- Edit or execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems.

- Exploit network devices, security devices, and/or terminals or environments using various methods or tools.
- Facilitate access enabling by physical and/or wireless means.
- Identify potential points of strength and vulnerability within a network.
- Maintain situational awareness and functionality of organic operational infrastructure.
- Operate and maintain automated systems for gaining and maintaining access to target systems.
- Conduct cyber activities to degrade/remove information resident in computers and computer networks.
- Process exfiltrated data for analysis and/or dissemination to customers.
- Provide real-time actionable geolocation information.
- Record information collection and/or environment preparation activities against targets during operations designed to achieve cyber effects.
- Test and evaluate locally developed tools for operational use.
- Test internal developed tools and techniques against target tools.
- 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.**