

DEPARTMENT OF
DEFENSE, VETERANS AND EMERGENCY MANAGEMENT
Military Bureau
Headquarters, Maine National Guard
Camp Keyes, Augusta, Maine 04333-0033

28 January 2016

TECHNICIAN POSITION VACANCY ANNOUNCEMENT #16-014

POSITION: Information Technology Specialist (InfoSec) (D2179P01) GS-2210-09
EXCEPTED POSITION

LOCATION: 101st Communications Flight, Bangor, Maine

SALARY RANGE: \$55,670 to \$72,366 per annum **GS-09**

CLOSING DATE: 12 February 2016

AREA OF CONSIDERATION:

AREA I - All permanent and indefinite Enlisted Technicians in the Maine Air National Guard.

AREA II – All Enlisted members of the Maine Air National Guard.

PERMANENT CHANGE OF STATION (PCS): PCS expenses may not be authorized for this position. Authorization for payment of PCS expenses will be granted only after a determination is made that payment is in the best interest of the Maine National Guard.

DUTIES: See attached duties and responsibilities.

MINIMUM QUALIFICATION REQUIREMENTS: Each applicant must show how they meet the Minimum Requirements and Specialized Experience listed below; otherwise, the applicant may lose consideration for this job.

SPECIALIZED EXPERIENCE: Must have twenty-four (24) months of experience which required the applicant to acquire and apply each of the following knowledge, skills, and/or abilities.

GS-09

1. Ability to conduct COMPUSEC/COMSEC training.
2. Knowledge of Network Security Best Practices.

3. Knowledge of the COMSEC and EMSEC Programs.
4. Knowledge of the Information Assurance Programs.
5. Knowledge and skill to conduct effective security reviews of new or existing systems and networks and to recommend revised or new measures based upon accreditation reviews or new equipment fielding requirements.

ADDITIONAL REQUIREMENT: The position is an IAM level 2 position. As a condition of employment, individuals have 6 months in which to complete and receive the SEI 267 (for the level and grade at which the person is serving) mandated by DoD Career Development Program for Information Assurance Workforce Improvement Program (DoD 8750.01M).

OTHER REQUIREMENTS: MUST POSSESS OR BE ELIGIBLE TO OBTAIN AND MAINTAIN A TOP SECRET SECURITY CLEARANCE.

COMPATIBILITY CRITERIA: 3D0X1, 3D0X2, 3D0X3, 3D1X1, 3D1X2, 3D1X3, 3D1X4
NOTE: If you do not possess the compatible AFSC, you will not be disqualified from being considered. Selected applicant must be prepared to attend the appropriate school.

MILITARY ASSIGNMENT: 3D0X3

SUBSTITUTION OF EDUCATION FOR SPECIALIZED EXPERIENCE: At the GS-9 level, a masters or equivalent graduate degree or 2 full years of progressively higher level graduate education leading to such a degree may be substituted.

SELECTED RESERVE INCENTIVE PROGRAM (SRIP): Non-Technician Maine National Guard personnel who are SRIP participants (bonus recipients/student loan repayment program) may have their benefits terminated and/or recouped if selected as a permanent military Technician. Applicants should contact the MeANG Incentive Manager Norman Stanton, MSgt DSN - 698-7391 to determine any possible termination and/or recoupment actions that may result from accepting this position.

HOW TO APPLY: Detailed instructions are contained in an Instruction Guide titled "Technician Vacancy Announcement Guide" which should be posted with this vacancy announcement. Applicants may apply using the OF Form 612 Optional Application for Federal Employment, a resume, or any other format they choose. In addition to their basic application, applicants are strongly encouraged to complete ME Form 171, Military Experience and Training Supplement. Applications forwarded to HRO should be no more than eight (8) pages although additional pages may be submitted as necessary. Applications should include written or documented proof of education, training, and work experience deemed necessary to adequately respond to general and specialized experience factors listed in the TPVA. Professional licenses or education transcripts necessary to validate qualifications should be submitted as required in the TPVA. Do not include photo copies of awards (a military ribbon rack or civilian certificate), letters of commendation, enlisted or officer performance reports, Technician performance

appraisals, and personal photos unless specifically requested in the TPVA. Applications must be forwarded to: Joint Force Headquarters, ATTN: HRO, Camp Keyes, Augusta, Maine 04333-0033, NOT LATER THAN the closing date. Applications received AFTER the closing date WILL NOT BE CONSIDERED. The use of government envelopes, postage or facsimile machines to submit applications is prohibited. We are allowed to receive facsimiles sent from non-government facsimile machines. The inter-office distribution system may be used. You may also e-mail it to: ng.me.mearng.list.hro-applications@mail.mil

APPOINTMENT: Selectee will be required to participate in Direct Deposit/Electronic Funds Transfer as a condition of employment. The Adjutant General retains exclusive appointment authority for Technicians. No commitment will be made to any nominee prior to a review of qualifications by this office. The Maine National Guard is an Equal Opportunity Employer. All appointments and promotions will be made without regard to race, color, creed, sex, age or national origin.

DISSEMINATION: Supervisors, please post to bulletin boards, read at unit formations and notify personnel who may be interested. Qualified personnel who may be absent during this announcement period due to ADT, AT, TDY, school, illness, etc., should be notified.

WORK: DSN 626-6013/COM (207) 430-6013 FAX: DSN 626-4246/COM (207) 626-4246

FOR THE HUMAN RESOURCES OFFICER:

///S\\
LISA M SESSIONS
MAJ, EN
Human Resources Specialist
(Recruitment & Placement/Compensation)

This position is located in the Operations Section of a Base Communications Unit. This is an Air National Guard (ANG) Dual Status Technician position requiring military membership, compatible military skill assignment, and classification. The purpose of this position is to serve as an assistant to the base Information Assurance Specialist and to administer the Communication-Computer Security (COMPUSEC) program, Electronic Key Management System (EKMS), Emission Security, and Information Assurance Awareness Programs.

MAJOR DUTIES:

1. Administers the COMPUSEC Program and protects Information Technology (IT) assets against unauthorized, accidental, or deliberate modification, disclosure, and destruction of data. Utilizes knowledge of IT principles, methods and security regulations and policies to carry out established base-wide policy to administer the INFOSEC (also known as COMPUSEC) program. Conducts risk assessments to identify possible security violations by analyzing computer assets and establishing security requirements based on possible countermeasures to achieve an optimum level of security. Executes and analyzes the effectiveness of computer security plans and enforces mandatory access control techniques such as trusted routers, bastion hosts, gateways, firewalls, or other methods of information systems protection. Performs program and system test plans devised to test for illegal input and unauthorized access. Assists in developing contingency plans designed for computer security emergency response, backup, and recovery operations. Assists all base organizations in the development of their individual INFOSEC program. Disseminates information and ensures computer security practices are adhered to by all functional areas. Carries out activities leading to security certification and accreditation (C&A) including providing guidance and assistance in the preparation of certification and accreditation packages. Processes and monitors all requests by contractor personnel to visit unit facilities. (25%)

2. Administers the Network Security Program. Maintains required information assurance certification IAW DoD 8570.01-M, Federal Information Security Management Act of 2002, Clinger Cohen Act of 1996. Implements procedures to ensure protection of information transmitted to the installation, among organizations on the installation, and from the installation on the local or wide area networks, the World Wide Web, or other communications modes. Utilizes current and future multi-level security products collectively to provide data integrity, confidentiality, authentication, non-repudiation, and access control of the LAN (Local Area Network). Reports all incidents involving viruses, tampering, or unauthorized system entry to appropriate authority. Carries out information technology (IT) security to prevent the penetration of computer systems for espionage, sabotage, or fraudulent purposes. Implements methods to prevent or minimize direct access, electronic or other forms of eavesdropping, interpreting electro-mechanical emanations, electronic intercept, telemetry interpretation, and other techniques designed to gain unauthorized access to IT information, equipment, or processes. Recognizes such potential, defines vulnerabilities, selects appropriate security measure from many acceptable alternatives and mitigates risks by overseeing the installation of physical and technical security barriers to prevent others from improperly obtaining such information. Conducts the Information Assurance Awareness Program, which uses computer-based

training for both initial and recurring information protection training. Maintains required course records. (25%)

3. Administers the Communications Security (COMSEC) program. Controls and protects all cryptographic material and administers the Cryptographic Access Program (CAP). Safeguards and controls all COMSEC equipment entered into the COMSEC Management Control System, keying material, COMSEC information, and other COMSEC-related functions. Receives, inventories, issues, transfers, destroys and inspects COMSEC material. Conducts security investigations or advises investigative appointees, as appropriate. Interprets and applies regulations/directives; develops cryptographic plans; determines new COMSEC requirements; and assures proper disposition of excess COMSEC materials including key. Furnishes written guidance to user accounts concurring effective dates, accounting procedures, destruction requirements, and physical security of COMSEC materials including key. Conducts semi-annual functional reviews of all COMSEC user accounts, inspecting COMSEC facilities, reviewing procedures, and auditing of all cryptographic holdings. Operates the Certification Authority Workstation. Prepares Emergency Action Plans to ensure that plans can be implemented immediately. Responsible for preparing, coordinating, and maintaining AFCOMSEC Forms 9 in the granting and withdrawing of cryptographic access. (20%)

4. Administers the Electronic Key Management System (EKMS) or Key Management Infrastructure (KMI) program. This includes system configuration and operation of the Local Management Device, Data Transfer Device, and Key Processor. Initializes the system, performs system backups, determines operator access, and control functions (privilege management), reloads and configures the operating system's parameters. Installs local COMSEC account hardware and software, including training alternates in the EKMS or KMI operations. Serves as secure voice (e.g., STE, Secure VoIP) User Representative and Emissions Security Program Administrator. Develops, implements, and monitors security systems for the protection of controlled cryptographic cards, documents, ciphers, devices, communications centers, and equipment. (20%)

5. Adheres to management control plan requirements by conducting self inspection and staff assistance visits. Resolves identified discrepancies. (10%)

6. Performs other duties as assigned.