

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

26 June 2014

TECHNICIAN POSITION VACANCY ANNOUNCEMENT #14-075

***** TEMPORARY PROMOTION *****

NOTE: Incumbent selected may be non-competitively promoted permanently.

POSITION: Information Technology Specialist (INFOSEC)(D2178000) (GS-2210-11)
EXCEPTED POSITION

LOCATION: 101st Communications Flight, Bangor, Maine

SALARY RANGE: \$59,932 to \$77,912 per annum

CLOSING DATE: 14 July 2014

AREA OF CONSIDERATION:

AREA I - All permanent and indefinite Enlisted (**E7 and Below**) Technicians in 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 General and Specialized Experience listed below; otherwise, the applicant may lose consideration for this job.

GENERAL EXPERIENCE: Technical, analytical, supervisory, or administrative experience which has demonstrated the candidates ability to analyze problems of organization, workforce, information requirements, etc. and provide systematic solutions; and the ability to deal satisfactorily with others.

SPECIALIZED EXPERIENCE: Must have thirty six (36) months experience for GS-11, which required the applicant to acquire and apply each of the following knowledge, skills, and/or abilities:

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 present 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: AFSC: 3D1X1, 3D1X2, 3D1X2 **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: A maximum of 12 months of the required experience may be substituted by successful completion of undergraduate study in an accredited college or university at the rate of 30 semester hours for 12 months of experience. The education must have been in a computer related field such as computer science, data processing, or information processing science. **Applicant must provide a copy of transcripts to receive credit. Must provide a copy of a transcript to receive consideration of substitution.**

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 626-6017 / COM (207) 430-6017 FAX: DSN 626-4246 / COM (207) 626-4246

FOR THE HUMAN RESOURCES OFFICER:

//s//

CRAIG P. BAILEY
MSG, MEARNG
Human Resources Specialist
(Recruitment & Placement/Compensation)

|

|

INTRODUCTION:

This position is located in the plans and resources flight of a base Communications Squadron. The purpose of this position is to serve as the base Information Assurance manager who is the wing commander's authority and focal point for Information Assurance. Manages the communication-computer security (COMPUSEC) program, electronic key management system (EKMS), emission security, and Information Assurance Awareness programs.

MAJOR DUTIES:

1. Serves as the wing Information Assurance Manager. Applies Information Technology (IT) security principles, methods, and security products to protect and maintain the availability, integrity, confidentiality, and accountability of information system resources and information processed throughout the system's life cycle. Establishes and publishes base-wide policy to manage the INFOSEC (also known as COMPUSEC) program and provides advice and guidance in its implementation and in procedures used in the development and operation of systems. 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. Reviews, analyzes, and validates certification and accreditation (C&A) packages. Continuously identifies and analyzes threats and vulnerabilities to the information systems to maintain an appropriate level of Protection. Ensures computer software designs address information system security requirements. Accomplishes risk analysis, security testing, and certification due to modifications or changes to computer systems. Evaluates, assesses, or locally tests and approves all hardware, software, and firmware products that provide security features prior to use on any accredited information system or network. Certifies all software prior to installation and use on communications and computer systems. Executes computer security plans and enforces mandatory access control techniques such as trusted routers, bastion hosts, gateways, firewalls, or other methods of information systems protection.
2. Manages 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 and advises on IT security policies and procedures to ensure protection of information transmitted to the installation, among organizations on the installation, and from the installation using local area networks (LAN), wide area networks (WAN), 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. Reports to MAJCOM, Air Force Communications Agency, National Security Agency, and Air Force computer emergency response team all incidents involving viruses, tampering, or unauthorized system entry. Controls access to prevent unauthorized persons from using network facilities. Limits access to privileged programs (i.e., operating System, system parameter and configuration files, and databases), utilities, and security-relevant programs/data files to authorized personnel. 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. Evaluates unusual circumstances to recognize and define potential vulnerabilities and selects and oversees 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.

3. Serves as the Communications Security (COMSEC) manager for all cryptographic activities including managing the cryptographic access program (CAP). Formulates and develops communications security criteria and requirements for inclusion in mobility, contingency, and exercise plans. Maintains accountability for sensitive cryptographic materials and related COMSEC information. Oversees issuance of COMSEC materials. Maintains COMSEC inventory. Prepares and evaluates written plans for emergency actions and ensures personnel are fully qualified in the execution of plans. Investigates COMSEC security incidents to determine the possibility of compromise to COMSEC materials and ensures documentation and reporting to appropriate channels. Performs destruction, receiving, issuing transferring and inspecting COMSEC material within the most stringent timelines. Furnishes written guidance to user accounts concurring effective dates, accounting procedures, destruction requirements, and physical security of COMSEC materials including key. Performs semi-annual functional reviews of all COMSEC user accounts, physically inspecting the user's COMSEC facilities, reviewing procedures, and audit of all cryptographic holdings. Manages the certification authority workstation. Manages the CAP by conducting briefings prior to granting access to cryptographic information. Documents cryptographic access certificates and acts as liaison for scheduling polygraph examinations of personnel enrolled in the program.

4. Implements and manages the electronic key management system (EKMS) 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 or oversees installation of local COMSEC account hardware and software, including training alternates in the AFEKMS operations. Serves as secure voice equipment (e.g., STE, secure VOIP) user representative and emissions security program manager. Develops, implements, and monitors security systems for the protection of controlled cryptographic cards, documents, ciphers, devices, communications centers, and equipment.

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

6. Performs other duties as assigned.