Position Announcement:

Title 5 - SUPERVISORY IT CYBERSECURITY SPECIALIST (INFOSEC) SAPF - ISSM

Overview

- Job Ad Closes: 09/30/2024
- Pay Grade: GS-2210-13, Title 5
- PD: NGT5893000
- Location: Burlington IAP, South Burlington, VT, 05403
- Salary $ 105,312-136,909 per year
- Area of Consideration-United States Citizens

Summary

The Vermont Air National Guard is hiring a civilian Title 5 GS-13 Supervisory IT Cyber Security Specialist (INFOSEC) for the Special Access Program- Facility (SAP-F) Branch of an Air National Guard (ANG). The position is permanent and is within the Advanced Programs Office (CCZ), as part of the 158th Fighter Wing in South Burlington, VT. The incumbent will serve as the Information Systems Security Manager (ISSM) under the supervision of the Program Manager and Deputy Program Manager of Wing Advanced Programs.

This is an excepted appointment with Permanent tenure.

Major Duties

- Serves as the principal advisor to the Wing Commander and Director of Advanced Programs on the latest industry and technological projections as they pertain to SAP Cyber Security/Information Security for the network enclave infrastructure. Develops policies for organization deployed throughout the Wing. Must anticipate the effects of new emerging technology and develop policies to control it to prevent security violations. Duties include oversight and accreditation of all systems IAW with all NGB, Air Force, and DOD security directives, policies and procedures. Ensures that all elements are in compliance with guidance concerning accreditation of automated information systems, risk management, control of computer viruses, and other similar issues. Ensures that security incidents are investigated and reported IAW with all command, Air Force, NGB and DOD security directives, policies and procedures. This includes auditing of IT systems, technical reviews, and ensuring proper IT Sanitization procedures are complied with IAW DOD security directives.

- Provides leadership, guidance, and direction to ensure acquisition, development, and retention of a professional, highly capable SAP cyber security workforce to accomplish assigned missions. Provides supervision in the daily operations for security activities for the enclave. Coordinates the work of team members to ensure that short-term and long-term goals and objectives are met. Directs, manages, and monitors a system of internal controls that ensure effective and appropriate use of resources.

- Establishes performance standards and evaluates employee performance. Reviews and recommends approval of candidates for promotions and recognition. Reviews and approves work plans to be accomplished by subordinates; priorities and schedules for completion of work; sets broad objectives; monitors subordinate employees' performance

in providing IT services; reviews accomplishments; and takes appropriate action of correction when deficiencies are noted. Gives advice, counsels, or instructs individual employees, on both work and administrative matters. Develops and evaluates performance standards; recommends and approves awards; hears and resolves group employee grievances or serious employee complaints. Reviews and makes decisions on serious disciplinary actions involving employees and makes decisions on work problems presented by subordinates. Initiates recognition and disciplinary actions for personnel. Identifies and arranges for appropriate training and development opportunities. Determines and approves training needs and establishes formal training plans.

- ISSM responsibilities include (taken from Joint SAP Implementation Guidance and AFI 17-101):

  A. Implementation of the RMF. Maintain and report IS and IT systems assessment and authorization status and issues in accordance with DoD Component guidance. Provide direction to the ISSO(s) in accordance with DoD, Air Force and NGB directives. Coordinate with the organization's cybersecurity service provider to ensure issues affecting the organization's overall security are addressed appropriately. Maintain a repository for all organizational or system-level Cybersecurity-related documentation. Ensure that ISSO(s) are appointed in writing and provide oversight to ensure they are following established Cybersecurity policies and procedures.
  B. Monitor compliance with cybersecurity policy, as appropriate, and review the results of such monitoring. Ensure that Cybersecurity inspections, tests, and reviews are synchronized and coordinated with affected parties and organizations. Ensure implementation of IS security measures and procedures including reporting incidents to the AO and appropriate reporting chains and coordinating system-level responses to unauthorized disclosures in accordance with DoD, Air Force, and NGB guidelines. Ensure handling of possible or actual data spills of classified information resident in ISs, are conducted in accordance with applicable guidelines.
  C. Act as the primary cybersecurity technical advisor to the Information System Owner (ISO) for DoD IS and IT systems under their purview. Ensure that Cybersecurity-related events or configuration changes that may impact DoD IS and IT systems authorization or security posture are formally reported to the AO and other affected parties, such as IOs and stewards and AOs of interconnected DoD ISs. Ensure the secure configuration and approval of IT below the system level (i.e., products and IT services) in accordance with applicable guidance prior to acceptance into or connection to a DoD IS or IT system.

- Collaborates with other supervisors and managers within the Wing and command to negotiate, decide on, or coordinate work-related changes affecting their operations. Advises their supervisor with broader and higher responsibilities on problems involving the relationship of the work of the cybersecurity teams to broader programs, and its impact on IT Services. Serves as a technical advisor to management. Participates as a member and advisor on special committees and special projects designed to study methods to enhance the use of IT throughout the Wing and command. Participates in command and Wing initiatives developing strategic plans for enhancement of the system environment, developing functional and technical requirements for acquisitions, conducting cost-benefit analyses, feasibility studies, and related activities. Maintains liaison with manufacturers and vendors, professional organizations, and counterparts at

other Wings/installations and services regarding available products and state-of-the-art technologies and advancements. Develops strategies to incorporate into the organization's inventory such technologies and advancements found to be compatible with user requirements, taking into consideration any affect these technologies and techniques will have on existing architecture and infrastructure. Participates in plans for acquisition and implementation of new equipment, including development of contract documentation. May serve as the contractor's liaison/consultant, providing technical advice and support throughout the acquisition, installation, and maintenance stages. Plans and schedules the installation of new or modified hardware, operating systems, and software applications. Considers factors such as compatibility, conversion or implementation costs, and impact on existing equipment. Advises Wing on issues pertaining to operating systems and hardware status.

- Performs other duties as assigned.

Conditions of employment

- Be a U.S. Citizen
- Must have a SECRET clearance but must be able to obtain a TOP SECRET with SCI eligibility within 6 months of employment.
- Incumbent must complete appropriate training and obtain required certifications IAW DoDI 8140,DOD 8570.01M or applicable governing document(s) for Cyber workforce as an IA Manager LevelII. All certifications are required within 6 months of employment.
- The employee must have and maintain a valid driver's license.
- Irregular and overtime hours may be required.
- May be required to travel by car, in military, and/or commercial aircraft for temporary duty assignments.
- Position is designated as OM-ADM-001 within the Defense Cybersecurity Workforce as guided by NIST SP 800-181; National Initiative for Cybersecurity Education, Cybersecurity Workforce Framework. Which establishes the Tasks, Skills, Knowledge, and Abilities expected of this position. (https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center).

SPECIALIZED EXPERIENCE GS-13:

Must have at least one (1) year of specialized experience equivalent to the GS-12 level that approaches techniques and requirements appropriate to an assigned computer applications area or computer specialty area in an organization. Experience planning the sequence of actions necessary to accomplish the assignment where this entailed coordination with others outside the organizational unit and development of project controls. Experience that required adaptations of guidelines or precedents to meet the needs of the assignment. Experience preparing documentation on cost/benefit studies where is involved summarizing the material and organizing it in a logical fashion. Experience in managing the function of the work to be performed. Experience which includes leading, directing and assigning work of personnel.

Evaluation

Applicants will be evaluated on the extent they meet or exceed the qualifications and demonstrate the core competencies. Applicants will also be evaluated on their oral communication; ability to work as part of a team; their potential to work with limited instruction in a fast-paced environment; and ability to utilize attention to detail.

How to Apply

The POC for this position is MSgt Alex Putnam, Deputy Program Manager, 158 Fighter Wing. Direct all questions and applications to him by email at alex.putnam@us.af.mil. All applications must include:

- A resume documenting professional experience with a cover letter
- Proof of professional IT Certification
- Other Documents will be required if selected