|  |  |
| --- | --- |
| **ADVERTISEMENT TRADITIONAL GUARD ENLISTED VACANCY ANNOUNCEMENT** | |
| **NEW YORK AIR NATIONAL GUARD**  **224TH AIR DEFENSE GROUP**  **366 OTIS STREET**  **ROME, NEW YORK 13441** | **ANNOUNCEMENT #:** FY 23-16 A-B |
| **DATE: 16 DEC 2022** |
| **CLOSING DATE: UNTIL FILLED** |
| **UNIT:** 224TH SUPPORT SQUADRON | **AFSC:** 1D751  **RANK:** SSGT |
| **POSITION TITLE:**  **CYBER DEFENSE OPS** | **AREA OF CONSIDERATION: NATIONWIDE**  All members who meet the qualifications for these positions. ALL MEMBERS ELIGIBLE TO JOIN THE AIR NATIONAL GUARD |
| **SPECIALTY SUMMARY**  AFECD 31OCT22  Manages and performs Defensive Cyber Operations (DCO) and cyber functions (DoDIN operations) in garrison and in deployed environments. Surveys, secures, protects, defends, preserves, designs, builds, operates, and extends data,  networks, net-centric capabilities, and other designated systems. This Air Force Specialty Code description incorporates the use of DoD Cyber Workforce Framework (DCWF) Codes to tie this specialty description to the framework. The DCWF was developed by the National Institute of Standards and Technology (NIST) and the DoD to establish a common lexicon and model for all cyber work. The DCWF will universalize training and education between academia, industry, and military. It will also enable talent management by ensuring the right Airmen, for the right assignment, at the right time. | |
| **DUTIES AND RESPONSIBILITIES**  2.1. Responds to disruptions within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness,  along with response and recovery approaches to maximize survival of life, preservation of property, and information security.  Investigates and analyzes relevant response activities and evaluates the effectiveness of and improvements to existing practices.  [DCWF Code – 531]  2.2. Tests, implements, deploys, maintains, reviews, and administers the infrastructure hardware, software, and documentation that are  required to effectively manage network defense resources. [DCWF Code – 521]  2.3. Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or  might occur within the network in order to protect information, information systems, and networks from threats. Uses data collected from  a variety of cyber defense tools (e.g., Intrusion detection system alerts, firewalls, network traffic logs.) to analyze events that occur  within their environments for the purposes of mitigating threats. [DCWF Code – 511]  2.4. Conducts threat and vulnerability assessments and determines deviations from acceptable configurations or policies. Assesses the  level of risk and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.  Performs assessments of systems and networks within the Network Environment (NE) or enclave and identifies where those  systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth  architecture against known vulnerabilities. [DCFW Code – 541]  2.5. Collects, processes, preserves, analyzes, and presents computer-related artifacts in support of network vulnerability mitigation  [DCWF Code – 211] | |
| **CLEARANCE**  Secret, as a minimum.  (SEE REVERSED) | |
| **INQUIRIES ABOUT POSITIONS**  **Please Contact The Recruiting Office @ 1800-883-4484 For Qualification and Eligibility Questions.**  **(This number rings on all recruiting phones)** | |