

**109 AW Airlift/Cybersecurity
Vacancy Announcement
(DSG Enlisted)**

**NEW YORK AIR NATIONAL GUARD
109th AIR NATIONAL GUARD BASE**

109th Airlift Wing
Stratton Air National Guard Base
Scotia, NY 12302-9752

UNIT: 109th Communications Squadron
Stratton ANGB Scotia, NY 12302-9752

MAX AVAILABLE GRADE: SSgt (E-5)

POSITION TITLE: Cyber Security

ANNOUNCEMENT NO:

DSG03-FY26

DATE:

24 September 2026

CLOSING DATE:

Until Filled

AFSC:

1D7X5

AREA OF CONSIDERATION: NATIONWIDE:

All Traditional Guardsman (includes technicians) who meet the
basic qualifications for this position.

[Anyone Eligible To Join The New York Air National Guard](#)

SPECIALTY SUMMARY *(As outlined in the current AFECD – 30APR2026)*

Cybersecurity secures, defends, and preserves data, network, net-centric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place, and taking internal security actions to protect DoDIN systems to execute DAF operations. Performs risk management framework security determinations of fixed, deployed, and mobile information systems (IS) and telecommunications resources to monitor, evaluate, and maintain systems, policy, and procedures to protect clients, networks, data/voice systems, and databases from unauthorized activity. Identifies potential threats and manages resolution of communications security incidents. Enforces national, DoD and Air Force security policies and directives to ensure Confidentiality, Integrity, and Availability (CIA) of Information Systems (IS) resources. Operations include identifying, locating, and validating vulnerability mitigation to prevent the compromise of the communications, information, electromagnetic environment, or industrial systems through protective measures. Oversees and governs the overall cybersecurity program to include Information Security (INFOSEC), TEMPEST, Communications Security (COMSEC), Emissions Security (EMSEC), and Computer Security (COMPUSEC) programs. This includes access to system controls, monitoring, administration, and integration of cybersecurity into all aspects of engineering and acquisition of cyberspace capabilities. DCWF work roles associated with this specialty will be list in the Career Field Education and Training Plan (CFETP).

DUTIES AND RESPONSIBILITIES *(IAW the current AFECD – 30APR2026)*

2.1. Conducts cybersecurity risk management framework assessments; ensures enterprise cybersecurity policies fully support all legal and regulatory requirements and ensures cybersecurity policies are applied in new and existing IS resources. Identifies cybersecurity weaknesses and provides recommendations for improvement. Monitors enterprise cybersecurity policy compliance and provides recommendations for effective implementation of IS security controls. Defends, protects, and secures mission networking environments and devices. Provides networked application resources by designing, configuring, installing, and managing data services, operating system, and server applications.

2.2. Evaluates and assists IS risk management activities. Makes periodic evaluation and assistance visits, notes discrepancies, and recommends corrective actions. Audits and enforces the compliance of cybersecurity procedures and investigates security-related incidents to include COMSEC incidents, classified message incidents, classified file incidents, classified data spillage, unauthorized device connections, and unauthorized network access. Develops and manages the cybersecurity program and monitors emerging security technologies and industry best practices while providing guidance to unit-level Information Assurance (IA) Officers. Employ countermeasures designed for the protection of confidentiality, integrity, availability, authentication, and non-repudiation of government information processed by AF IS's.

2.3. Responsible for cybersecurity risk management of national security systems during all phases of the IS life cycle through remanence security.

2.4. Integrates risk management framework tools with other IS functions to protect and defend IS resources. Advises cyber systems operations personnel and system administrators on known vulnerabilities and assists in developing mitigation and remediation strategies. Provides CIA by verifying cybersecurity controls are implemented in accordance with DoD and Air Force standards. Ensures appropriate administrative, physical, and technical safeguards are incorporated into all new and existing IS resources and protects IS resources from malicious activity.

2.5. Performs COMSEC management duties in accordance with national and DoD directives. Maintains accounting for all required physical and electronic cryptographic material. Issues cryptographic material to units COMSEC Responsible Officer (CRO). Provides guidance and training to appointed primary/alternate CRO. Conducts inspections to ensure COMSEC material is properly maintained and investigates and reports all COMSEC related incidents.

2.6. Performs TEMPEST duties in accordance with national and DoD TEMPEST standards. Denies unauthorized access to classified, and in some instances, unclassified information via compromising emanations within a controlled space through effective countermeasure application. Ensures all systems and devices comply with national and DoD EMSEC standards. Inspects classified work areas, provides guidelines and training, maintains area certifications, determines countermeasures; advises commanders on vulnerabilities, threats, and risks; and recommends practical courses of action.

2.7. Responsible for oversight or management of installation cybersecurity awareness programs. Promotes cybersecurity awareness through periodic training, visual aids, newsletters, or other dissemination methods in accordance with organizational requirements.

2.8. As part of the Warfighter Communications career field, performs IT project management duties to include managing, supervising, and performing planning and implementation activities. Manages implementation and project installation and ensures architecture, configuration, and integration conformity. Develops, plans, and integrates base communications systems. Serves as an advisor at meetings for facility design, military construction programs, and minor construction planning. Evaluates base comprehensive plan and civil engineering projects. Monitors the status of cyber or communications-related base civil engineer work requests. Performs mission review with customers. Controls, manages, and monitors project milestones and funding from inception to completion. Determines adequacy and correctness of project packages and amendments. Monitors project status and completion actions. Manages and maintains system DAFECD, 30 Apr 26

70

installation records, files, and indexes. Evaluates contracts, wartime, support, contingency and exercise plans to determine impact on manpower, equipment, and systems.

QUALIFICATIONS AND SELECTION FACTORS:

3.1. Knowledge. Knowledge of the following is mandatory. IS resources; capabilities, functions and technical methods for IS operations; organization and functions of networked IS resources; communications-computer flows, operations and logic of electromechanical and electronics IS and their components, techniques for solving IS operations problems; and IS resources security procedures and programs including Internet Protocols.

3.2. Education. For entry into this specialty, completion of high school or general educational development equivalency is mandatory. Additional courses or certifications in computer and information systems technology are desirable. Any network or computing commercial certification is desirable.

TO INQUIRY ABOUT THIS or ANY 109TH AIRLIFT WING POSITIONS:

**Please Contact The 109th Recruiting Office @ 518-344-2201 or
109aw.airwing.recruiting@us.af.mil, with any Qualification/Eligibility or
Vacancy Questions.**