DEPARTMENTS OF THE ARMY AND AIR FORCE

JOINT FORCE HEADQUARTERS-LOUISIANA
OFFICE OF THE ADJUTANT GENERAL
JACKSON BARRACKS
NEW ORLEANS, LOUISIANA 70117

Announcement Number: 26-043

POSITION TITLE:	AFSC	OPEN DATE:	CLOSE DATE:
Cybersecurity	1D775	20 May 2026	10 June 2026

UNIT OF ACTIVITY/DUTY LOCATION:
159th Communications Squadron, New Orleans, Louisiana

GRADE REQUIREMENT:
Min: E-5 **Max:** E-7

SELECTING SUPERVISOR:	Position Number
Capt Ryan T. Baldwin	1133241

AREAS OF CONSIDERATION

On-board LA ANG AGR (**Must hold *1D7X5 or *able to retrain**)
Louisiana Air National Guard members (**Must hold *1D7X5 or *able to retrain)**

MAJOR DUTIES

Please refer to attached pages for more info on the major duties and initial qualifications for this position for this AFSC or go to: https://www.my.af.mil to review the AFECD

INITIAL ELIGIBILITY CRITERIA

In addition to criteria listed on attached pages
- Security Clearance - Must attain and maintain: Top Secret

PREFERRED QUALIFICATIONS

In accordance with HRO and ANGI 36-101, the Selection Official has requested the following documents. While applications that do not include these documents will not be disqualified by HRO, their omission may negatively impact the selection process.

1. Cover Letter
2. Resume
3. Last three (3) EPBs / OPBs
4. Letter(s) of Recommendation

ACTIVE GUARD AND RESERVE REQUIREMENTS

AGR Program Entry and Tour Guidelines – LA ANG

- **Initial AGR Tours**: Initial tours with the Louisiana Air National Guard (LA ANG) may not exceed five (5) years. AGR tours cannot extend beyond an enlisted member's Expiration Term of Service (ETS) or an officer's Mandatory Separation Date (MSD).
- **Fitness Requirements:** Applicants must meet the minimum requirements in each fitness component and achieve a composite score of 75 or higher to qualify for entry into the AGR program. Members with a documented Duty Limitation Code (DLC) that prevents completion of one or more components of the Fitness Assessment must have an overall rating of "Pass."
- **Medical and Readiness Requirements:**
- Selected individuals must meet medical qualifications outlined in AFI 48-123, Medical Examination and Standards.
- Members must be current in all Individual Medical Readiness (IMR) requirements, including immunizations.
- RCPHA/PHA and dental exams must have been completed within 12 months prior to AGR tour start.
- An HIV test must be completed within six (6) months of the tour start date.
- **Overgrade Assignments:** Enlisted Airmen voluntarily accepting a position that results in an overgrade must submit a written voluntary demotion letter with their application, in accordance with ANGI 36-2503, Administrative Demotion of Airmen. The application package will not be processed without this documentation.
- **AFSC Qualification:** If the selected applicant does not currently possess the required AFSC, they must complete all required training and meet assignment criteria within 12 months of assignment. Failure to do so may result in termination of the AGR tour. Extensions beyond the 12-month period will be considered only if delays are beyond the applicant's control.
- **For additional details, please refer to ANGI 36-101, Active Guard Reserve Program.**

SPECIAL ANNOUNCEMENT CRITERIA

- Upon selection additional medical verification will be required prior to start of AGR tour
- Any Individual(s) selected for this position must meet EFMP requirements for the duty location at time of assignment.
- Members that do not meet EFMP standards for the duty location may be subject to a rescinded offer of employment.
- Continuation beyond initial tour may be subject to evaluation based on AGR Continuation Board
- Selection is not a promise of promotion

APPLICATION PROCEDURES

Applications must be signed and dated. Applications received with an unsigned NGB 34-1 will not be forwarded for consideration. Per ANGI 36-101, the application package must include at a minimum items 1-3 listed below. If the required documents are not submitted, a letter of explanation must be included. Incomplete packages will not be considered for the position vacancy:

1. **NGB Form 34-1** *(announcement number and position title must be annotated on the form)*
2. **CURRENT full Records Review RIP** from Virtual MPF https://vmpf.us.af.mil/vMPF/Hub/Pages/Hub.asp
3. **CURRENT PASSING Report of Individual Fitness** from MyFSS/MyFitness <(must not show a "fitness due date" that is in the past) (or) a signed letter from the UFPM. If exempt, please include Form 469 with application)
4. Items requested in the "PREFERRED QUALIFICATIONS ORDER" section above.

Application Documents Order:

- 1. (Mandatory) NGB Form 34-1
- 2. (Mandatory) Records Review RIP
- 3. (Mandatory) **Passing** Report of Individual Fitness
- 4. (Recommended) Cover Letter
- 5. (Recommended) Resume
- 6. (Recommended) Last three (3) EPBs / OPBs
- 7. (Recommended) Letter(s) of Recommendation

EMAILING REQUIREMENTS:

Consolidate all required documents into **ONE single PDF** (adobe portfolio is not accepted). To preserve signatures, consider printing signed documents to PDF before combining files. **Name the PDF file as follows: Last Name, Announcement Number, Position Title.**

Example: Doe, 26-XXX

Email Subject should be: Last Name, Announcement Number, Position Title

Example: Doe,26-XXX, Cybersecurity

Email Application Package to: **ng.la.laarng.mbx.agr-branch-air@army.mil**

** *There is a known issue that digital signatures are being removed from the NGB Form 34-1 once combined as one PDF. To avoid this, once you sign and save the NGB Form 34-1, go to Print, then select "Microsoft Print to PDF". Click Print. Use this copy of the form to combine into the required documents and send to HRO. Always verify the signature is present before you sent to HRO.* **

QUESTIONS: Applicants may call HRO for initial review of application and to verify receipt prior to closeout date. DSN 278-8753/8754 or Commercial 504-278-8753/8754 cassie.l.ellis.mil@army.mil / khisha.m.donald.mil@army.mil. Assistance will be rendered in the order the request was received.

INSTRUCTIONS TO COMMANDERS/SUPERVISORS: The selecting supervisor is responsible for contacting qualified applicants to schedule interviews. Once the Human Resources Officer (HRO) approves the selection package, the HRO will issue a notification letter to the Hiring Official. The Hiring Official is then responsible for notifying all applicants of their selection or non-selection. Please note: The selection is not considered final until the ANG AGR Manager has provided formal approval to the Hiring Official.

THE LOUISIANA NATIONAL GUARD IS AN EQUAL OPPORTUNITY EMPLOYER

All applicants are protected under Title VI of the Civil Rights Act of 1964. Eligible candidates will be considered without regard to race, color, religion, gender, national origin, or any other non-merit-based factor.

Note: Due to assignment restrictions in certain units and specific AFSCs/MOSs, some positions may have gender-specific requirements.

AFSC 1D775, Craftsman
AFSC 1D755, Journeyman
AFSC 1D735, Apprentice
AFSC 1D715, Helper

★CYBERSECURITY
(Changed 31 Oct 25)

1. **Specialty Summary**: 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 industrials 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).

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

3. ★**Specialty Qualifications.**
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.
3.3. ★Training. For award of the AFSC 1D735, completion of Cyber Surety initial skills course is mandatory.
3.4. Experience. The following experience is mandatory for award of the AFSC indicated:
3.4.1. 1D755. Qualification in and possession of AFSC 1D735. Experience performing cybersecurity functions and/or activities.
3.4.2. 1D775. Qualification in and possession of AFSC 1D755. Experience supervising cybersecurity functions and/or activities or resource and project management.
3.5. Other. The following are mandatory as indicated:
3.5.1. For entry into this specialty, see attachment 4 for entry requirements.
3.5.2. For award and retention of this AFSC:
3.5.2.1. ★Individual must maintain local network access IAW AFI 17-130, Cybersecurity Program Management and DAFMAN17-1301, Computer Security.
3.5.2.2. Specialty routinely requires work in the networking environment.
3.5.2.3. ★Must obtain or meet DoD Cyber Workforce qualifications based on approved cyberspace requirements applicable for cyberspace tasks required for any position held IAW DoDM 8140.03, *Cyberspace Workforce Qualification and Management Program*, and DAFMAN 17-1305, *DAF Cyberspace Workforce Management Program.*
3.5.2.4. Specialty requires routine access to Top Secret material or similar environment.
3.5.2.5. Completion of a current Tier 5 (T5) background investigation according to AFMAN 16-1405, Personnel Security Program Management, is mandatory.
3.5.2.6. Must maintain a Top-Secret clearance for retention of this AFSC.

NOTE: Award of the 3-skill level without a completed T5 investigation is authorized provided an interim Top-Secret security clearance has been granted according to AFMAN 16-1405