Announcement Number: 033-22

POSITION TITLE: Cyber Defense Operations
AFSC: 1D7X1E
OPEN DATE: 23 June 2022
CLOSE DATE: 13 July 2022
GRADE REQUIREMENT: Min: E-5 Max: E-7

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

SELECTING SUPERVISOR: Capt Alex Davenport
Position Number: 1080712

AREAS OF CONSIDERATION
On-board LA ANG AGR (Must Hold 1D7X1E AFSC)
Louisiana Air National Guard members (Must Hold 1D7X1E AFSC)

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*
- Must attain and maintain a minimum Information Assurance Technical Level II certification IAW AFMAN 17-1303, Cybersecurity Workforce Improvement Program and DoD 8570.01-M, Information Assurance Workforce Improvement Program, as specified by AFSC shredout: For 1D7X1E, a minimum Information Assurance Technical Level II certification.
- Completion of a background investigation according to AFMAN 16-1405, Personnel Security Program Management is mandatory by AFSC shredout specified: For 1D7X1E, completion of a current Tier 3 (T3), Secret

PREFERRED QUALIFICATIONS
In accordance with HRO and ANGJ 36-101, the following documents have been requested by the Selection Official. Applications received that do not contain these requested items will not be screened-out by HRO; but it may adversely affect the selection.

1. Cover Letter
2. Resume
3. Last three (3) EPRs / OPRs
4. Letter(s) of Recommendation
5. Copy of State Driver’s License (photocopy of both sides)
**ACTIVE GUARD AND RESERVE REQUIREMENTS**

Initial tours for the LA ANG may not exceed 5 years. AGR tours may not extend beyond an Enlisted member’s ETS or an Officer’s MSD. Airmen must meet the minimum requirements for each fitness component in addition to scoring an overall composite of 75 or higher for entry into the AGR program. For members with a documented Duty Limitation Code (DLC) which prohibits them from performing one or more components of the Fitness Assessment, an overall "Pass" rating is required. Individuals selected for AGR tours must meet the Preventative Health Assessment (PHA)/physical qualifications outlined in AFI 48-123, Medical Examination and Standards. They must also be current in all Individual Medical Readiness (IMR) requirements to include immunizations. RCPHA/PHA and dental must be conducted not more than 12 months prior to entry on AGR duty and an HIV test must be completed not more than six months prior to the start date of the AGR tour. Enlisted Airmen who are voluntarily assigned to a position which would cause an overgrade must indicate such in writing; a voluntary demotion letter must be included with the application in accordance with ANGI 36-2503, Administrative Demotion of Airmen, when assigned to the position. Acceptance of demotion must be in writing and included in the assignment application package. Application Package will not be forwarded without Administrative Demotion statement. If a selectee does not possess the advertised AFSC, he/she must complete the required training/assignment criteria within 12 months of being assigned to the position. Failure to do so may result in immediate termination. Extension past 12-months will only be considered if the delay is through no fault of the applicant. Any further questions regarding the AGR program may be answered in ANGI 36-101.

**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](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 UFPF. If exempt, please include Form 469 with application>

4. Items requested in the "PREFERED QUALIFICATIONS" section above.

**EMAILING REQUIREMENTS:**

Ensure all requirements are consolidated into **ONE single PDF** (adobe portfolio is not recommended) (consider printing signed documents to PDF prior to combining files)-Signatures may be stripped once they are saved. PDF File Name should be: Last Name, Announcement Number

Example: Doe, XXX-22

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

Example: Doe, XXX-22, Personnel

Email Application Package to: ng.la.laarg.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 or Commercial 504-278-8753 or cassie.l.ellis.mil@army.mil. Assistance will be rendered in the order the request was received.

**INSTRUCTIONS TO COMMANDERS/SUPERVISORS:** Selecting supervisor will contact qualified applicants for interviews. After the Human Resources Officer HRO approves the selection package, the HRO office will send a notification letter to the Hiring Official who will in turn notify all applicants of their selection non-selection. The selection of an applicant is not final until the Hiring Official has been notified by of approval by ANG AGR Manager.

**THE LOUISIANA NATIONAL GUARD IS AN EQUAL OPPORTUNITY EMPLOYER**

All applicants will be protected under Title VI of the Civil Rights Act of 1964. Eligible applicants will be considered without regard to race, color, religion, gender, national origin, or any other non-merit factor. Due to restrictions in assignment to certain units and AFSC MOS some positions may have gender restrictions.
1. **Specialty Summary.** Manages and performs Defensive Cyber Operations (DCO) and cyber support functions (DoDIN operations) in-garrison and at deployed locations. 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.

2. **Duties and Responsibilities:**

2.1. Responds to disruptions within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and 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., IDS 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. Assess 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. [DCWF Code – 541]

2.5. Collects, processes, preserves, analyzes, and presents computer-related artifacts in support of network vulnerability mitigation [DCWF Code – 211]

2.6. Performs and supports cyber mission Planning, Briefing, Execution, and Debriefing (PBED). Identifies, validates and synchronizes resources to enable integration during the execution of defensive cyber operations. [DCWF Code - 332]

2.7. Oversees the cybersecurity program of an information system or network; including managing information security implications within the organization, specific program, or other area of responsibility, to include Communications Security (COMSEC), Emissions Security (EMSEC), Computer Security (COMPUSEC), personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources. Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives. [DCWF Code 612/722/723]

2.8. Installs, configures, troubleshoots, and maintains server and systems configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Administers server-based systems, security devices, distributed applications, network storage, messaging, and performs systems monitoring. Consults on network, application, and customer service issues to support computer systems’ security and sustainability. [DCWF Code – 451]

2.9. Manages and administers integrated methods, enabling the organization to identify, capture, catalog, classify, retrieve, and share intellectual capital and information content. The methods may include utilizing processes and tools (e.g., databases, documents, policies, procedures) and expertise pertaining to the organization. [DCWF Code – 431]

2.10. Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices. Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results. Works on the development phases of the system development lifecycle. Makes daily product decisions, works on a collaborative team, pairs with team members, and helps ensure user satisfaction using Lean and Agile methodologies. Works with the project team, leadership, stakeholders, and other PMs to progress the goal of shipping the right product to users. Ensures that the product is successful in terms of user value, stakeholder value, and organizational business goals. [DCWF Code – 621/622/632]

2.11. Consults with stakeholders to guide, gather, and evaluate functional and security requirements. Translates these requirements into guidance to stakeholders about the applicability of information systems to meet their needs. [DCWF Code - 641]

2.12. Develops, administers, and secures databases, data management systems, and/or data processes for the storage, query, and utilization of data. Examines data from multiple disparate sources with the goal of providing new insight. Designs and implements custom algorithms, flow processes and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes. Locates patterns in large data sets using computer science techniques to help team members with different levels of
understanding and expertise to make data driven business decisions that increase effectiveness or efficiency of operational forces. [DCWF Code – 421/422]

2.13. Provides end users tiered-level customer support by coordinating software, hardware, and network configuration, troubleshooting, resolution, security, maintenance, and training. [DCWF Code – 411]

3. **Specialty Qualifications:**

3.1. Knowledge. Knowledge is mandatory of principles, technologies, capabilities, limitations, and cyber threat vectors of servers, clients, operating systems, databases, networks and related hardware and software, cybersecurity principles including: national and international laws, policies, and ethics related to operational cybersecurity; operational risk management processes; and specific operational impacts of lapses in cybersecurity.

3.2. Education. For entry into this specialty, completion of high school or general educational development equivalency is mandatory. Additional courses in Science, Technology, Engineering, and Mathematics (STEM) are desirable. Associate degree or higher in related fields and/or Information Technology (IT) certification is desirable.

3.3. Training. For award of the 1D731X, completion of the suffix-specific course is mandatory.

3.4. Experience. The following experience is mandatory for award of the AFSC indicated:

3.4.1. There are no specific upgrade requirements for the slick AFSC 1D7X1 not already defined in the training AFI.

3.4.2. For award of the 1D751X, qualification in and possession of 1D731X and experience in suffix specific functions.

3.4.3. For award of the 1D771X, qualification in and possession of 1D751X and experience in suffix specific functions.

3.4.4. For award of the 1D791, qualification in and possession of 1D77XX and experience managing and directing cyber defense activities.

3.5. Other. The following are mandatory as indicated:

3.5.1. For entry into this specialty:

3.5.1.1. See attachment 4 for additional entry requirements.

3.5.2. For award and retention of these AFSCs:

3.5.2.1. Must attain and maintain a minimum Information Assurance Technical Level II certification IAW AFMAN 17-1303, Cybersecurity Workforce Improvement Program and DoD 8570.01-M, Information Assurance Workforce Improvement Program, as specified by AFSC shredout:

3.5.2.1.1. For 1D7X1, a minimum of position requirements.

3.5.2.1.2. For 1D7X1A, a minimum Information Assurance Technical Level II certification.

3.5.2.1.3. For 1D7X1B, a minimum Information Assurance Technical Level II certification.

3.5.2.1.4. For 1D7X1D, a minimum Information Assurance Management Level I certification.

3.5.2.1.5. For 1D7X1E, a minimum Information Assurance Technical Level II certification.

3.5.2.1.6. For 1D7X1K, a minimum of position requirements.

3.5.2.1.7. For 1D7X1R, a minimum of position requirements.

3.5.2.1.8. For 1D7X1Z, a minimum of position requirements.

3.5.2.2. Must maintain local network access IAW AFI 17-130, Cybersecurity Program Management and AFMAN 17-1301, Computer Security.

3.5.2.3. Completion of a background investigation according to AFMAN 16-1405, Personnel Security Program Management, is mandatory by AFSC shredout specified:

3.5.2.3.1. For 1D7X1,

3.5.2.3.2. For 1D7X1A, completion of a current Tier 5 (T5), Top Secret.

3.5.2.3.3. For 1D7X1B, completion of a current Tier 5 (T5), Top Secret.

3.5.2.3.4. For 1D7X1D, completion of a current Tier 5 (T5), Top Secret.

3.5.2.3.5. For 1D7X1E, completion of a current Tier 3 (T3), Secret.

3.5.2.3.6. For 1D7X1K, completion of a current Tier as specified by position requirements.

3.5.2.3.7. For 1D7X1R, completion of a current Tier 3 (T3), Secret.

3.5.2.3.8. For 1D7X1Z, completion of a current Tier 5 (T5), Top Secret.

**NOTE:** Award of the 3-skill level without a completed Tier 5 Investigation is authorized provided an interim Top Secret clearance has been granted according to AFMAN 16-1405.

4. **Specialty Shredouts:**

<table>
<thead>
<tr>
<th>Suffix</th>
<th>Portion of AFS to Which Related</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Network Operations</td>
</tr>
<tr>
<td>B</td>
<td>Systems Operations</td>
</tr>
<tr>
<td>⚫D</td>
<td>Security Operations</td>
</tr>
<tr>
<td>⚫E</td>
<td>Client Systems Operations</td>
</tr>
<tr>
<td>⚫K</td>
<td>Knowledge Operations</td>
</tr>
<tr>
<td>R</td>
<td>RF Operations</td>
</tr>
<tr>
<td>Z</td>
<td>Software Development Operations</td>
</tr>
</tbody>
</table>