



Information Technology (IT) security developments, and of the infrastructure protection environment to select appropriate tools to be used by team members. Establishes methodology and determines best techniques to secure computer systems and to protect cyber key terrain from exploitation of information within these systems and/or to achieve other tasked objectives in cyberspace. Leverages knowledge of multiple entities with a stake in current operations to plan and build appropriate courses of action and training scenarios. Functions in at least one of the following advanced roles:

2.1.1. Cyberspace Crew Commander. Develops tactical objectives and/or tactical taskings for a team of Cyberspace Operators. Serves as the liaison between assigned team and other teams or external entities.

2.1.2. Cyberspace Operations Controller. Directs tactical execution for a team of Cyberspace Operators. Develops tactical approach and synchronizes actions of multiple qualified operators in order to achieve objectives.

2.1.3. Operations Planner/Scheduler. Represents the unit's capability, availability, and interests at high-level Operational Planning Team (OPT) meetings to define the mission, environment, enemy, effects, capabilities, overall plan, phasing, operational agreements and contingencies needed to conduct the operation or exercise. Develops a tactical plan for assigned missions and exercises. Works as a member of the mission leadership element to translate operational objectives into tactical objectives comprised of specific tactical tasks. Develops Measures of Effectiveness and Measures of Performance to be used in the assessment of the mission's or exercises success. Prepares and coordinates operator, resource, facilities and equipment schedules in coordination with unit and flight commanders in order to ensure training, currency, and mission timelines and objectives are met.

2.1.4. Industrial Control Systems (ICS) Cyberspace Operator. Assesses and evaluates vulnerabilities and/or adversary activity in ICS enclaves. Detects, characterizes, and resolves insecurities in ICS networks. Reviews and analyzes ICS network traffic, configurations, and operating procedures and provides recommendations to improve system security posture.

2.2. Conducts extensive research of new vulnerabilities and insecurities discovered in operating systems, application software, infrastructure and boundary protection devices. Investigates, analyzes, and develops methods that could be used to exploit these vulnerabilities. Conducts testing on training range to validate findings and to develop and refine methods and procedures to mitigate vulnerabilities. Coordinates research and findings with the Cyberspace Weapons Officer for inclusion in unit and cyberspace community tactics, techniques, and procedures.

2.3. Prepares Unit Training Assembly, Annual Training and currency training events for Mission Ready Cyberspace Operators to optimize training time available. Ensures training for each event has been prepared and is ready. Monitors assigned military members' go-no-go readiness status and ensures deficiencies are recognized. Works with scheduling section to provide opportunities for assigned members to maintain full mission readiness. Coordinates with maintenance section to ensure all assigned equipment is in good working condition and ready for each training and mission event.

2.4. Performs other duties as assigned.

**★3. Specialty Qualifications:**

3.1. Thorough knowledge of the mission, objectives, terminology, and management practices in the activity, the agency and the department to recognize probable areas of interaction and to serve as a technical expert in systems/network security.

3.1.1. Thorough knowledge of network systems design, development, testing, installation, operating, management, and maintenance concepts and methods to provide and protect network services.

3.1.2. Knowledge of, and skill in applying IT security principles and methods and of IT security products and services sufficient to evaluate and recommend the acquisition of, implement, and disseminate IT security tools, procedures, and practices to protect information assets.

3.1.3. Extensive knowledge of information technology methods and information protection techniques and procedures. This includes government and Commercial-Off-The-Shelf (COTS) technology using industry standards and an ability to understand the capabilities and limitations of software, utility programs, network management systems and programming.

3.1.4. Knowledge of hardware, software, and operating systems; systems configuration and integration; maintenance, upgrades, and modifications.

3.1.5. Extensive knowledge of hardware, software, network operations functions, firewalls, packet switching communications protocols, and diagnostic tools to analyze difficult and complex system problems and provides resolutions.

3.1.6. Knowledge of systems analysis, configuration management, and computer equipment requirements related to networks to assess vulnerabilities. Skill in evaluating innovative approaches in formulation of programs or systems specifications.

3.2. Education. Not used.

3.3. Training. For award of AFSC 1B491, completion of the Cyberspace Superintendent Course is mandatory.

3.4. SC 1B471 is mandatory.

3.5. Other.

3.5.1. Specialty requires routine access to Top Secret material or similar environment. For award and retention, completion of a current Single Scope Background Investigation (SSBI) according to AFI 31-501, *Personnel Security Program Management*, is mandatory. Must also maintain DoD 8570.1 IAM Level II certification.

3.5.2. For award and retention of these AFSCs, must maintain an Air Force Network License according to AFI 33-115, Vol 2, *Licensing Network Users and Certifying Network Professionals*.

**4. Remarks.**

4.1. All questions regarding this announcement should be directed to MSgt Lisa Silvis at commercial (210) 925-6996 or DSN: 945-6996.

**SUBMIT APPLICATIONS TO:** 149 FSS/FSMPM  
ATTN: MSGT LISA SILVIS  
107 Hensley St., Ste 2  
San Antonio, TX 78236-0103

**NOTE: ALL HARDCOPY APPLICATIONS MUST BE RECEIVED IN THIS OFFICE BY CLOSE OF BUSINESS, **1600 HOURS**, ON THE CLOSE OUT DATE. APPLICATIONS WILL NOT BE TAKEN ELECTRONICALLY. THOSE THAT DO NOT MAKE THE DEADLINE WILL NOT BE CONSIDERED AND RETURNED WITHOUT ACTION.**