**Job Title:** Journeyman Cybersecurity Engineer

**Class:** Full Time at Redstone Arsenal Al

**Position Description:**

The Journeyman Cybersecurity Engineer will be a key member of a team performing Foreign Military Sales (FMS) Equipment and Software Cybersecurity Systems Engineering along with key functions supporting the Risk Management Framework (RMF) Assessment and Authorization (A&A) process for tactical systems.

The candidate will have the following responsibilities:

* Provide accurate technical evaluations of the FMS equipment, software applications, full system, or network and documenting the security posture, capabilities, and vulnerabilities against applicable NIST controls.
* Selecting and implementing security controls, timely completion of accreditation packages, formulating and implementing mitigations and maintaining the security posture of systems.
* Identify, assess and mitigate system security threats/risks throughout a system’s lifecycle, validate system security requirements, formulate and maintain documentation and system certification and accreditation activities (planning, testing, assessing and coordinating).
* Responsible for leading cybersecurity process/tool improvements.
* Monitoring and evaluating a system's compliance with Department of Defense (DoD) security, resilience, and dependability requirements including performing validation steps, comparing actual results with expected results and analyze the differences to identify impact and risks at the software application, system, and network levels.
* Work with team to provide solutions and to ensure continued functionality of systems within DoD RMF Framework
* Additional duties as assigned

**Basic Qualifications:**

* Degree: Bachelor’s Degree (Information Technology or Cybersecurity) with 3 to 10 years of experience.
* Experience with implementing and evaluating DoD STIG requirements, NIST RMF, IAVMs and Cybersecurity assessment tools (ACAS, Nessus, SCC, STIG Viewer)
* Knowledge of the Risk Management Framework (RMF) process and NIST security controls.
* Security Control Assessor-Validator (SCA-V) experience.
* Experience with Confluence and Jira.
* Knowledge of information system architecture and standards as they apply to cyber security
* Sec+ or higher certification
* Ability to travel. Travel will be estimated around than 25% per year.

**Other Qualifications**

* Master’s Degree preferred (Information Technology or Cybersecurity)
* Experience in a DoD security environment preferred
* Candidates should have strong communication and writing skills; be able to work in a team-oriented environment supporting a diverse customer base comprised of program managers, engineers, analysts, specialists, and technicians; and strong attention to detail.

**Security Requirements:**

Candidate must be a US Citizen and possess (and be able to maintain) a Final Secret Clearance or meet the eligibility to obtain (and maintain) a Secret Clearance.