**Job Title:** Product Cybersecurity Engineer – Protected Tactical Enterprise System (PTES) (Level 4/5/6)

**Job Location:** Colorado Springs, Colorado

**Security Clearance:** SECRET

**Clearance Status:** Must be Obtainable

---

**Job Summary:**

Responsible for a wide range of product cybersecurity engineer responsibilities associated with the Protected Tactical Enterprise Service (PTES) project. A successful candidate contributes to developing next-generation technology in an agile environment. The candidate should have experience as a lead cybersecurity engineer in a continuous development/continuous integration (CI/CD) pipeline, working within the Department of Defense (DOD) Risk Management Framework (RMF), ability design and implement security controls and countermeasures, evaluate remediation recommendations, and employ system security processes and methods.

PTES is a next-generation military satellite communications (MILSATCOM) system that manages and transmits the protected tactical waveform (PTW). PTES uses the PTW to provide secure, anti-jam communications over Wideband Global SATCOM (WGS) satellites and terminals. This capability will ensure the user can receive required services over SATCOM resources in benign, contested, degraded, and operationally limited (CDO) environments.

---

**Required Qualifications:**

- DOD 8570 IAT Level II Certification
- 5+ years of experience with Information Systems Security
- Proficiency in design and development in an Agile environment
- Experience decomposing complex requirements into epics and user stories
- Strong teamwork and interpersonal skills
- Excellent verbal, written, communication, and interpersonal skills
- Ability to work independently as well as within a team

**Preferred Qualifications:**

- Current U.S. Government SECRET security clearance (required U.S. Citizenship)
- Prior experience with an Agile/Scrum team using Jira/Confluence/Maven/Jenkins is highly desirable
- Experience with Wideband Global SATCOM (WGS) and protected SATCOM systems, products, and interfaces
- Technical interface with internal and external stakeholders
- Experience preparing, statusing, and presenting detailed schedules, technical material, and readiness review data both verbally and written
- Ability to coordinate tasks, provide clear task status, address risk issues, and resolve issues across multiple groups

- Familiarity with other engineering disciplines (systems, hardware, test, configuration management, and quality engineering) and how they interact with software engineering
- Penetration testing and vulnerability management experience
- Experience with ACAS, STIG Viewer, and CIS Control Implementation/checks

**Educational Requirements:**

- *Engineer Level 4*: Bachelor's degree and 12+ years of experience, Master's with nine or more years of experience
- *Engineer Level 5:* Bachelor's degree and 14+ years of experience, Masters's with 12+ years of experience, Doctorate with 9+ years of experience
- *Engineer Level 6:* Bachelor's degree and 20+ years of experience, Masters's with 18+ years of experience, Doctorate with 15+ years of experience

(Degrees must be from an accredited course of study in engineering, computer science, mathematics, or physics)

In compliance with Colorado's Equal Pay for Equal Work Act, the salary range for this position is $99,000 to $185,000. Ascension Engineering Group considers factors such as work experience, education, key skills, and position role when extending an offer.

Ascension Engineering Group is an Equal Opportunity/Affirmative Action Employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, pregnancy, sexual orientation, gender identity, national origin, age, protected veteran status, or disability status.