GreenDart

GPS Cybersecurity Engineer (Locations: CO or CA)

Description:

- Design and develop new systems, applications and solutions for the GPS enterprise-wide cyber systems and networks
- Ensure cyber compliance, perform security reviews and manage accreditation documentation
- Integrate new architectural features into existing infrastructures, design cyber security architectural artifacts, provide architectural analysis of cyber security features and relate existing system to future needs and trends
- Use forensic tools and techniques for attack reconstruction in order to resolve integration and testing issues
- Implement the Risk Management Framework accreditation process
- Support Air Force personnel in formulating responses to Higher Headquarters and Department of Defense requests for information and in assessing policy changes

Required Qualifications:

- 4 + years of Information Assurance (IA) or Cybersecurity (CS) experience
- Knowledge of IA/CS tools (e.g. Retina, SCAP, ACAS, Nessus and Kali Linux Security Suite)
- Able to obtain a DoD 8570.01M IA Management Level 1 within 180 days of start
- Familiar with the Risk Management Framework
- Strong written and oral communication skills
- Bachelor of Science in Computer Science, Computer Information Systems, Mathematics or Engineering
- Current DoD Secret security clearance

Highly Desired Qualifications:

- Defense Information Systems Agency (DISA) Security Implementation Guides (STIGs) and security controls experience
- Microsoft and UNIX/Linux Operating Systems experience
- Current certification(s) in CISSP, GPEN, GWAPT, GCIH, CEH, Network+, Security+, CCNA or CCNP
- Computer programming and database scripting experience