Embedded (Cyber Security) S/W Engineer

Location	Orlando, Florida
Work Arrangement	Full-Time, On-Site, 4/10A-1st Shift
Clearance	Active Secret Clearance

Grit Government Solutions is currently looking for an Embedded S/W Engineer for its customer based out of Orlando, Florida. This position is for real-time C/C++ embedded software engineers. This engineer will integrate with the program protection team to design, develop and integrate low-level firmware/software, and/or develop specialized cyber software solutions and tools based on mission requirements. Responsibilities include contributing to secure software development, performing security validation, and supporting threat mitigation efforts throughout the product lifecycle. This is cyber security engineering (embedded) position.

Required Qualifications:

- Active Secret Clearance or Active Interim Secret Clearance with most recent investigation in the last 5 years
- Bachelor's degree in Computer Engineering, Electrical Engineering, Computer Science or related field
- 3+ years of hands-on embedded real-time software development experience
- Proficient in C/C++ for embedded systems development
- Understanding of microcontroller architectures (ARM, RISC-V, etc.)
- Direct experience implementing security controls and in embedded environments (e.g., crypto, key management, secure boot, flash/partition encryption, memory protection units, side-channel mitigation)
- Hardware/software integration experience

Desired Qualifications:

- Direct experience implementing cryptographic algorithms and protocols in embedded firmware.
- Proven experience with embedded cryptographic key lifecycle management (generation, provisioning, storage, rotation, revocation, and sanitization)
- Knowledge of security frameworks/standards applied to embedded systems for cybersecurity and anti-tamper.
- Background in threat modeling, firmware/software vulnerability assessment, or secure product development lifecycle.
- Experience with use of software configuration management systems (e.g., Git, GitLab)
- Proficiency with embedded security toolchains (GDB, static/dynamic analysis)
- Familiarity with secure coding guidelines and safe memory management practices
- Experience with secure reprogramming/provisioning, update mechanisms, firmware signing, and chain-of-trust validation