



Cyber Analyst

Job Title: Cyber Analyst
Work Location: Alexandria, VA
Position Classification: Full Time
Security Clearance: Active SECRET clearance

Overview

Trident Technologies and Consulting - Global, LLC (d.b.a. T2C-Global) is currently seeking motivated and talented individuals who can offer the knowledge, skills, and experience to support the United States Navy, NAVSEA HQ in administrating Naval Expeditionary Programs (EXM) Professional Support Services program.

Responsibilities

The Cybersecurity Analyst serves as a subject-matter expert in Risk Management Framework (RMF) implementation and SysAdmin/ISSE for two to four individual Projects. This role is responsible for ensuring project adherence to US Navy RMF requirements, patching/hardening of project software, and generation of acquisition required IT documentation.

Duties Include

- Review cybersecurity policies, procedures, and directives to ensure compliance with DoN, DoD, and federal regulations (e.g., DoD 8500-series, NIST SP 800-series, Clinger Cohen Act, and various Defense Acquisition polices).
- Conduct and review system and program risk assessments to identify cybersecurity risks and provide strategies for remediation and mitigation.
- Lead strategic initiatives to strengthen cybersecurity projects' posture, balancing operational effectiveness with security imperatives.
- Partner with program managers, system engineers, and contractors to ensure cybersecurity is integrated throughout acquisition and development phases.
- RMF package development/implementation, and SysAdmin/ISSE support.

Required Qualifications

- **Active SECRET clearance**
- Bachelor's degree or higher from an accredited college or university in a cybersecurity-related field (can substitute with matching experience and certifications).
- 3-5 years' experience as a System Administrator/ISSE with ability and willingness to adhere to Privileged Access Agreement (PAA).
- Current member of DoD Cybersecurity Workforce (CSWF) per SECNAV M-5239.2 with necessary IA and OS certifications: Security +, Windows 10-11, Linux (Redhat, Ubuntu).
- In depth knowledge of system administration tasks of isolated/standalone DoD systems running Linux (preferably Ubuntu) and Windows to include offline OS upgrades, security patches, software installation.
- Experience with maintaining system baselines to include imaging and deployment tools, processes and procedures.
- Demonstrated experience in RMF package development/implementation.
- In depth knowledge of RMF (NAVSEA) processes and procedures
 - RMF Process Guide (RPG)
 - Standard Operating Procedures (SOP's)
 - Business Rules
 - SCA Risk Assessment Guide
 - RMF templates
 - DISN CPG
- Demonstrated knowledge to perform the official functions of SA/ISSE
 - Implementation of NIST 800-53 Controls in eMASS
 - STIG implementation
 - Generation and maintenance of POA&M in eMASS



- Vulnerability Assessment to include mitigation and mitigating factors
- Document creation and management
 - System Security Plans
 - Hardware/Software Lists
 - Architecture and Design Drawings (using Visio)
 - SLCM Strategy
 - Standard Operating Procedures
 - Configuration Guides
- Current eMASS account.

Desired Qualifications

- ACAS certification and training necessary to configure, update, manage and maintain Tenable.io/Security Center and Tenable Nessus systems
- Familiarity with DITPR/DADMS
- Working knowledge of Cybersecurity tools necessary for artifact creation
 - STIG viewer
 - Evaluate STIG
 - eMASSter
- Certification in a relevant Cybersecurity field (e.g., CISSP, CISM, GLSC, CASP+)..

Supplemental Information

Special Conditions

- If offered employment, you will be required to submit to a background investigation.
- Employees performing sensitive requirements must be able to pass a drug test as a condition of employment and submit to random drug testing throughout the contract performance period as per FAR 252.223-7004, Drug Free Workforce. If your position requires drug testing to successfully meet contractual obligations, this will be a condition of employment.

Equal Opportunity Employment Statement

T2C-Global is an equal employment opportunity employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, gender, national origin, disability status, protected veteran status or any other characteristic protected by law.

T2C-Global Point of Contact

If interested in applying for the above listed position, please contact us at; recruiter@t2cglobal.com