



Senior Cybersecurity Analyst

Job Title: Senior Cybersecurity 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 Senior Cybersecurity Analyst serves as a subject-matter expert in Cybersecurity Policy, Planning, and Risk Management Framework (RMF) implementation. This role is responsible for tracking the status of Authority To Operate (ATOs) and other Risk Management Framework (RMF) functions, reviewing, analyzing, and interpreting cybersecurity policies, while also guiding and tracking the integration of cybersecurity engineering principles throughout system lifecycles. The incumbent will act as a trusted consultant to leadership, bridging the gap between compliance requirements, operational readiness, and technical solutions.

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).
- Advise program leadership on emerging cybersecurity directives, regulatory and statutory changes, and policy impacts to mission systems.
- Monitor and track system authorization (ATO) efforts under the NAVSEA Risk Management Framework and provide early warnings of issues or when progress may be off track.
- Monitor and track various data calls for compliance in accordance with specific directives (OPORD, TASKORD, etc.).
- 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 posture across programs, balancing operational effectiveness with security imperatives.
- Represent the program office in high-level working groups, interagency forums, and technical exchanges.
- Partner with program managers, system engineers, and contractors to ensure cybersecurity is integrated throughout acquisition and development phases.
- Participate in the change management process, including conducting security impact analyses and making recommendations to program management for approvals.

Required Qualifications

- **Active SECRET clearance**
- Bachelor's degree or higher from an accredited college or university in a cybersecurity-related field.
- Minimum 8–10 years of progressively responsible experience in cybersecurity policy, compliance, and engineering.
- Demonstrated experience with DoN/DoD cybersecurity programs, RMF, and secure systems engineering.
- Proven track record of reviewing policy documents, advising leadership, and implementing engineering solutions.
- Strong understanding of Navy acquisition processes and mission systems.
- Ability to translate complex technical requirements into actionable policy.
- Exceptional communication, negotiation, and stakeholder engagement skills.
- Proficiency in vulnerability management, system hardening, and secure configuration.
- Proven leadership in cross-functional cybersecurity initiatives.



Desired Qualifications

- Certification in a relevant Cybersecurity field (e.g., CISSP, CISM, GLSC, CASP+).
- Self-starter who is willing to both take the lead and provide support in a team role in a complex, fast-paced, cross-disciplinary work environment.
- Strong organization skills with the ability to quickly turn around requests.
- Flexible and readily adaptable to changing responsibilities.
- Ability to engage stakeholders and collaborators across various DoD agencies and services.
- Ability to attend and organize program reviews/site visits/field tests.

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