Trident Technologies and Consulting – Global, LLC

Risk Management Framework (RMF) Information Systems Security Officer (ISSO)

Job Title: **RMF ISSO**
Work Location: **Albany, GA**
Position Classification: **Full Time**
Security Clearance: **Active SECRET clearance**

Overview

Trident Technologies and Consulting - Global, LLC (d.b.a. T2C-Global) is a SBA Certified Woman Owned Small Business (WOSB) and Certified Woman Owned Florida Business Enterprise specializing in providing innovative global defense services and solutions.

T2C-Global is currently seeking motivated and talented individuals who can offer the knowledge, skills, and experience as for our Albany, GA based customer. This is a pre-award effort, and the position is contingent upon contract award.

Responsibilities

Provide, sustain, and enhance Cybersecurity Support Services (CSS) to include: 1) Assessment and Authorization (A&A)/Risk Management Framework (RMF) validation services; 2) A&A/RMF package support from cradle to grave; 3) vulnerability management, to include monitoring, tracking, and reporting; and 4) Cybersecurity (CY) daily operational support for MARCORLOGCOM G6's Information Technology (IT) Portfolio of Information Systems. Provide technical expertise to support ongoing cybersecurity responsibilities delineated by activity. Provide reportable metrics for Information Systems (System A&A, POA&M, Annual Security Control Testing, Annual Security Review, Annual Contingency Plan Testing), to the MARCORLOGCOM ISSM in order to meet the Federal Information System Management Act (FISMA) reporting requirements.

Specific duties include:

- Complete authorization and assessment packages within 120 days of system ATO expiration.
- Ensure stakeholders are kept informed of risk, status, and roles and responsibilities throughout the RMF process.
- Guide information owners through completion of Step 0 System Registration in Marine Corps Compliance and Authorization Support Tool (MCCAST).
- Guide information owners through Step 1, System Categorization, in MCCAST based on information provided by the information owner IAW ECSM 018, FIPS Publication 199 and NIST SP 800-60.
- Guide information owners through Step 2, select security controls. Determine appropriate defense level and appropriate overlays.
- Provide information owner with an export of the MCCAST selected security controls and applied overlays to populate the Implementation Details.
- Review completed security control implementation details and gain validator approval before uploading into MCCAST for ISSM submission for an Initial Risk Assessment (IRA).
- 5Mmanage MCCAST entries updates on behalf of the ISSM and information owners assisting with preparation and review of Federal Information Security Management Act (FISMA) documentation.
- Guide information owners in the development of a System Security Plan (SSP) that addresses objectives for the assessment, methods for verifying security control compliance, the schedule for the initial control assessment, and actual assessment procedures.
- Work with ISSM and lead Government RMF ISSO to conduct the initial assessment of the effectiveness of the security controls and document the issues, findings, and recommendations in a Security Assessment Report (SAR).

- Develop a project plan and accompanying Plan of Action and Milestones (POA&M) for the RMF package that addresses all un- remediated vulnerabilities, failed Security Technical Implementation Guideline (STIG) failures and failed security controls. Contractor shall develop and report metrics that include the percentages of completion in every step of the RMF process.
- Work the POA&M with the ISO and shall include all elements required by MCCAST. Update the POA&M at least monthly for the life cycle of the IS using the latest vulnerability scans and STIG checklists.
- Attend scheduled and ad-hoc Cybersecurity branch meetings for update and coordination of cyber and RMF efforts.
- Continuously monitor the IS IAW existing and emergent Continuous Monitoring policies.
- Initiate RMF package creation NLT 12 months from current IS Authority to operate expiration date.
- Maintain all RMF artifacts and documents in the designated Government repository.
- Provide support and technical expertise related to Defense in Depth principles and technology in security engineering designs and implementation.
- Document and report cybersecurity audit findings and recommendations for each system to the PM and ISSM.
- Provide continuous feedback in the form of lessons learned to the Government to ensure process and practices remain efficient and effective.

Qualifications

- **Current DoD Active SECRET clearance**
- Information Assurance Technician (IAM) Level II professional.
- Bachelor's degree (Preferred)
- A minimum of 5 years' experience
- Must be familiar with the use of the Marine Corps Compliance and Authorization Support Tool (MCCAST).
- Must be familiar with the use of the Assured Compliance Assessment Solution (ACAS) scanning tool.

Physical Demands

The physical demands described here are representative of those that must be met by an employee to successfully perform the essential functions of the job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions. While performing the duties of this job, the employee is required to reach with hands and arms. The employee is frequently required to sit, stand, and walk. The employee may be required to move ten pounds and could occasionally lift or move up to twenty-five pounds.

Disclaimer: The listed duties are not intended to serve as a comprehensive list of all duties performed by all employees in this classification, only a representative summary of primary duties and responsibilities. Incumbent(s) may not be required to perform all duties listed and may be required to perform additional position specific duties.

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 a Veteran friendly employer and provides equal employment opportunity (EEO) to all employees and applicants without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, age, disability status, genetic information, marital status, ancestry, protected veteran status, or any other characteristic protected by applicable federal, state, and local laws. Equal Opportunity for VEVRAA Protected Veterans. T2C-Global will not discriminate against employees and job applicants who inquire about, discuss, or disclose compensation information.

T2C-Global POINT OF CONTACT

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