1934 Old Gallows Road, Suite 350
Tysons, VA 22182
703.226.8018
zentekconsulting.com

Position Title: IA Security Specialist

Start Date: July 1, 2017 (Tentative - based on anticipated award)

Clearance Requirements: Active DOD Secret

Location: Fort Meade, MD

Travel: Minimal

Job Description:

- Perform information assurance and system security support for multiple systems in accordance with Federal regulations & standards (FISMA, NIST, etc.) and DOD policy and guidance, to include:
  - Secure architecture design and review
  - NIST RMF Assessment & Authorization (A&A) support, to include required documentation development
  - Security Plan of Actions and Milestones (POA&M) development
  - Mitigation strategy development for findings that cannot be fixed immediately
  - IAVA review and compliance support
  - Audit inquiry and response support
  - FISMA/NIST/FedRAMP requirements and process advisement
- Prepare reports and presentations as required

Skills:

- Experience developing, assessing, reviewing, and updating A&A documentation to satisfy NIST RMF and FISMA requirements for DOD Federal Agencies, to include:
  - Assigning IA controls based on Mission Assurance Category (MAC) and Confidentiality Level (CL)
  - Initiating the ATO Implementation Plan
  - Developing and maintaining System Security Plans, Security POA&Ms, Validation Results, and artifacts associated with implementation of IA controls
  - Performing Security Impact Assessments on system change requests
  - Managing FISMA artifacts in a system of record (e.g. eMASS)
  - Recommending, implementing, and validating corrective actions identified in the Security POA&M
- Ability to identify organizational security weaknesses in logical security controls; physical security controls; personnel controls; operational security; training, incident and emergency response; and with the integrity of software applications and data

- Ability to understand vulnerability assessment results and analysis on networks, servers, websites, databases, applications, and assist with other assessment activities
- Ability to review vulnerability findings, identify mitigations, and prepare Findings and Remediation Reports
- Must possess a detailed knowledge of security regulations (FISMA, NIST, FIPS, etc.) and guidance to include:
    - DoDD 8500.1: Information Assurance (IA)
    - DoDI 8500.2: Information Assurance (IA) Implementation
    - DoDI 8510.01P: Risk Management Framework for DoD Information Technology (IT)
    - DISA DAA Vulnerability Management Policy Memo, Dec 18, 2013
- Experience preparing reports and presentations required for communicating findings and recommended solutions, to include:
    - Vulnerability Assessment Reports and Matrices, STIG Checklists and Compliance Reports, IAVA Compliance Reports, POA&Ms and related Risk Acceptance Documentation, Diagrams (Logical network diagrams detailing communications paths, ports, protocols, management traffic, and encryption) and Component Documentation Reports.
- Proficient with Microsoft Office suite of products
- Excellent presentation, written, and verbal communication skills

Education /Certification Requirements:

- DOD 8570 IAT I
    - 0 to 5 or more years of experience in IA technology or a related field
    - At least one (1) of the following baseline certifications:
        - Cisco CCNA-Security
        - CompTIA A+
        - CompTIA Network+
        - ISC(2) System Security Certified Practitioner (SSCP)
- DOD 8570 IAT II
    - At least 3 years in IA technology or a related area
    - At least one (1) of the following baseline certifications:
        - Cisco CCNA-Security
        - CompTIA Security+
        - GIAC Global Industrial Cyber Security Professional (GICSP)
        - GIAC Security Essentials Certification (GSEC)
        - ISC(2) System Security Certified Practitioner (SSCP)
- DOD 8570 IAT III
    - At least 7 years' experience in IA technology or a related area
    - At least one (1) of the following baseline certifications:
        - CompTIA Advanced Security Practitioner (CASP)
        - ISACA Certified Information Systems Auditor (CISA)
        - ISC (2) Certified Information Systems Security Professional (CISSP)
        - GIAC Certified Enterprise Defender (GCED)
        - GIAC Certified Incident Handler (GCIH)