# AVUM Cybersecurity Specialist

**Position Summary**

Avum is seeking an Information Assurance Specialist to support cybersecurity, compliance, and risk management activities across Federal and Department of Defense (DoD) programs. This individual will help ensure information systems meet security requirements, maintain compliance with government regulations, and support the protection of sensitive and classified information.

The ideal candidate has experience supporting cybersecurity programs, conducting security assessments, managing system accreditation activities, and working within Federal security frameworks. This role will partner closely with system administrators, engineers, program managers, and security stakeholders to maintain a strong security posture across mission critical environments.

**Key Responsibilities**

- Support information assurance and cybersecurity activities for Federal and DoD systems.
- Assist with the implementation and maintenance of security controls in accordance with NIST, RMF, and DoD requirements.
- Support system security authorization and accreditation efforts.
- Conduct security assessments, vulnerability reviews, and compliance evaluations.
- Monitor security findings and coordinate remediation activities with technical teams.
- Develop and maintain security documentation including System Security Plans (SSPs), POA&Ms, policies, and procedures.
- Assist with continuous monitoring activities and cybersecurity reporting requirements.
- Support security audits, inspections, and customer assessments.
- Evaluate system changes to ensure compliance with established security requirements.
- Work with stakeholders to identify and mitigate cybersecurity risks.
- Support incident response and security investigations as needed.
- Stay current on evolving cybersecurity threats, regulations, and industry best practices.

**Compensation**

The salary range for this position is $110,000 – $145,000 annually. Actual compensation will be determined based on experience, qualifications, certifications, and geographic location. Avum offers a comprehensive benefits package including medical (Cigna), dental and vision (Principal), 401(k), PTO, education reimbursement, and certification reimbursement.

**Work Environment & Requirements**

- U.S. citizenship required
- Security clearance: Active Secret clearance required or ability to obtain
- Background investigation required

**Equal Employment Opportunity**

Avum, Inc. is an Equal Opportunity Employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, disability, veteran status, or any other protected class under federal, state, or local law. Avum is committed to compliance with Section 503 of the Rehabilitation Act and VEVRAA, and maintains an active Affirmative Action Plan.

**Required Qualifications**

- U.S. Citizenship with the ability to obtain and maintain a Secret Security Clearance.
- Bachelor's degree in Cybersecurity, Information Technology, Computer Science, Information Systems, or related field. Equivalent experience may be considered.
- 5+ years of experience supporting Information Assurance, Cybersecurity, or Information Security programs.
- Knowledge of NIST cybersecurity frameworks and Risk Management Framework (RMF) processes.
- Experience developing and maintaining security documentation.
- Experience supporting vulnerability management and security compliance activities.
- Understanding of security controls, risk management, and cybersecurity best practices.
- Strong analytical, organizational, and communication skills.

**Preferred Qualifications**

- Active Secret Security Clearance.
- Security certifications such as Security+, CISSP, CAP, CISM, or CASP+.
- Experience supporting Department of Defense programs and security requirements.
- Experience with eMASS, ACAS, SCAP, STIGs, or related cybersecurity tools.
- Familiarity with NIST 800-53, NIST 800-171, CMMC, and FedRAMP requirements.
- Experience supporting cloud security initiatives within AWS or Azure environments.
- Experience participating in Authority to Operate (ATO) efforts.