



## Cybersecurity Policy Administrator

**Description:** Cassidy Consulting Group is seeking a Cybersecurity Policy Administrator. This is a W-2 job opportunity. Please visit our website to learn more about Cassidy Consulting Group – <https://www.cassidyconsulting.us>.

### Job Responsibilities:

This position is for a Cybersecurity Policy Administrator/Information System Security Officer (ISSO) supporting hosted customers. ALTESS is a managed service provider (MSP) for Army IT systems. We support both on premises IT Systems as well as commercial cloud customers who reside in Microsoft Azure (Gov/DoD). We also provide sustainment services to support systems and applications. This position is for a cybersecurity policy administrator to support a full range of cybersecurity services for ALTESS customers.

### Position Requirements:

- Serve as subject matter expert on Cybersecurity Policy Administration.
- Work within Enterprise Mission Assurance Support Service (eMASS) to add and update documentation, import ACAS and STIG files, work with POA&Ms, and all other aspects of eMASS management.
- Work between technical and policy teams to implement, maintain, and monitor technical security configuration controls, including: STIGs, SRGs, and other industry security hardening guidance.
- Work between technical and policy teams to successfully implement and manage requirements for maintaining ATO and security control inheritance capabilities.
- Collaborate with internal and external parties to transform high-level technical objectives into comprehensive technical requirements.
- Act as the ISSO for hosted systems, assuming the responsibilities as outlined in AR 25-2.
- Assist hosted customers in obtaining and maintaining RMF for DOD IT and other certifications as required.
- Update and/or assist the hosted system's personnel in updating artifacts of the authorization package and store the artifacts in organizationally defined repository; i.e., system diagram (logical and physical) Hardware/Software/Firmware Inventory, Interface & Ports, Protocols and Services listing, etc.
- Assist in the preparation of network infrastructure specifications or designs incorporating required information security features.
- Review and evaluate Information Systems Design Plans, Continuity of Operation Plans, Communication Plans, engineering change proposals and configuration changes for compliance with relevant security regulations, policies, and best industry practice.
- Interact with the Army CSSP and customer ISSMs on a regular basis.

### Required Skills:

- Mid to senior level Cybersecurity Policy Administrator experience in an Army environment
- DoD 8570.01-M IAM level II certification is required
- Resource must possess Baseline certification as defined in DoD Instruction 8570.01-M
- eMASS experience required
- Strong verbal and written communication skills
- Experience effectively managing multiple large-scale projects
- Experience automating routine administrative tasks desired
- Understanding of network, storage, server, and application technologies



- Working knowledge of DoD STIGs, and IA Vulnerability Management (IAVM)

**Contract Labor Category, Education, & Experience:**

Information Assurance Engineer – Senior: Masters +10yrs, or Bachelors +12rs  
(Another on-site only in Radford)

**Security Clearance:** DOD Secret (Fully Adjudicated), as a minimum

**Citizenship:** United States

**Required Certifications:**

CompTIA Security+  
DoD 8570.01-M IAM level II certification

Cassidy Consulting Group is an Equal Employment Opportunity employer. Cassidy Consulting Group prohibits discrimination against employees and qualified applicants for employment on the basis of race, color, religion, sex (including pregnancy), age, disability, marital status, national origin, veteran status, or any other classification protected by applicable discrimination laws.