

## **ICF - Enterprise Cybersecurity & Resilience**

**Assessment and Authorization (A&A) Analyst - (3 total openings) – Req. # 170000041**

**Fort Lee, Petersburg VA**

**\$5000k Sign-on Bonus and relocation assistance available**

### **Job Description:**

The Assessment and Authorization (A&A) Analyst is responsible for planning, documenting, and conducting comprehensive security assessments using both the DOD Information Assurance Certification and Accreditation Process (DIACAP) and NIST Risk Management Framework (RMF). Additionally, the Analyst is responsible for reviewing existing documentation, IA controls, and DISA Security Technical Implementation Guideline (STIG) implementations

### **Key Responsibilities:**

- Performing comprehensive security assessments using the DOD Information Assurance Certification and Accreditation Process (DIACAP).
- Developing IT system security documentation as required by both the DIACAP and the NIST Risk Management Framework (RMF).
- Develop, maintain, and update the Plan of Action and Milestones (POA&M).
- Utilize knowledge of Mission Assurance Categories (MAC), Classification Levels (CL) and the 8500.2 IA controls associated with each level.
- Responsible for documentation review; reading over policy and procedures; Ports Protocols and Services Management (PPSM); system and network diagrams, descriptions, SOPs, previous certification and accreditation documents; compiling and generating deliverables (DIACAP scorecard, and findings).
- Reviewing IA Controls with the customer for specific applicability and compliancy.
- Conducting Security Tests and Evaluation (ST&E) for Accreditation or re-accreditation.
- Analyzing ST&E results; assess, determine, and describe risks associated with the results.
- Understanding of DISA Security Technical Implementation Guides (STIGs)
- Knowledge of DoD policies, regulations, and guidelines.
- Travel up to 10%.

### **Basic Qualifications:**

- Ability to maintain a DoD clearance.
- Bachelor's Degree or the equivalent combination of education, professional training, or work experience.

- DOD 8570 Compliance, or the ability to quickly obtain the security certifications: Security+, and CEH.
- Minimum of three (3) years C&A experience.
- Experience with the use of the DoD Vulnerability Management System (VMS) and Electronic Enterprise Mission Assurance Support Service (eMASS).
- Knowledge of Continuous Monitoring and Risk Scoring (CMRS), Host Based Security Systems (HBSS), and the Assured Compliance Assessment Solution (ACAS).
- Ability to demonstrate strong knowledge of computer security concepts.
- Demonstrated ability to document processes and procedures.

### **Preferred Skills/Experience:**

- Initiative and a personal interest in Information Technology Security.
- People skills, and the ability to communicate effectively with various clients with the ability to explain and elaborate on technical details.
- Certified Information Systems Security Professional (CISSP), Certified Authorization Professional (CAP), GIAC Systems and Network Auditor (GSNA).
- A strong understanding of DOD information assurance policy and regulations.

### **Professional Skills/Required Skills:**

- Excellent written and verbal communication skills.
- Excellent problem solving skills.

### **About ICF:**

ICF (NASDAQ:ICFI) is a global consulting and technology services provider with more than 5,000 professionals focused on making big things possible for our clients. We are business analysts, policy specialists, technologists, researchers, digital strategists, social scientists and creatives. Since 1969, government and commercial clients have worked with ICF to overcome their toughest challenges on issues that matter profoundly to their success. Come engage with us at [icf.com](http://icf.com).

Point of contact: **Thomas W. Houston** | **Cyber Security Recruiter** | +1.770-826-5329 mobile | [Tom.Houston@icf.com](mailto:Tom.Houston@icf.com)

**ICF** | Bldg 3, Corporate Square, Suite 370, Atlanta, GA