Cyber Security Engineer

Job Summary:
Terp Techs is seeking a Cyber Security Engineer to join our IT Security Engineering Team. The candidate will be responsible for working with agency and enterprise level stakeholders to plan, develop, and assist with the implementation of Assessment & Authorization (A&A) processes and the associated documentation. The candidate will be expected to provide expert A&A consultancy advocacy, offering recommendations on projects to ensure compliance with Federal regulations and standards and agency policies. In addition, the candidate must be able to work with stakeholders in functional and technical environments in support of IT security priorities. The individual should have strong communication skills and be willing to take initiative in a dynamic, collaborative, and client-facing environment.

Responsibilities:
- Assist with the transition from C&A or SA&A to A&A;
- Assist with compliance reviews and documentation for new or noncompliant systems including FIPS-199 system categorizations, E-Authentication risk assessments, Privacy Threshold Assessment, Privacy Impact Analysis, and Security Controls Assessments;
- Work with the Federal ISSOs to complete A&A artifacts including System Security Plans, Configuration Management Plans, Business Impact Analysis, Business Continuity Plans, and support the ATO process;
- Assist stakeholders in identifying and evaluating administrative, technical, and operational security risks, threats, weaknesses and vulnerabilities associated with information systems;
- Provide support to System, Information, and Data Owners and assist with Security Control integration and incorporation into the SDLC;
- Assist with development of security controls assessment and business continuity testing strategies;
- Provide cybersecurity technical advisory services regarding Federal and commercial leading practices, relevant strategic initiatives, and emerging technologies/trends; and
- Stay updated on Federal policies, regulations, FISMA compliance and standards, and Cyber Security requirements.

Requirements:
- Minimum 2 years of experience in a Federal Cyber Security environment
- At least 2 years of experience in Cyber Security policy development, FISMA standards, and C&A or A&A assessments
- Must have a Bachelors' Degree, preferably in Cyber Security, Information Systems, or Computer Science or a related field
- At least one IT Security or Cyber Security certification (Associate of $(ISC)^2$, SSCP, CISSP, CISA, Security +, etc.) is preferred or willingness to work toward a certification
- Deep understanding of compliance requirements, standards, and guidelines governing security within the Federal Government including FISMA, OMB Circular A-130, FIPS 199, FIPS 200, and the NIST Risk Management Framework

- Deep understanding of NIST Special Publications; specifically, 800-30, 800-37, 800-39, 800-53 Revision 4, 800-53A, 800-60, and 800-128
- Working knowledge of C&A or A&A processes
- Working knowledge of risk analysis and security controls assessments techniques
- Familiarity with the SDLC and how to properly implement security into the process
- Excellent oral and written communication skills

Terp Techs is an Equal Opportunity Employer.
EOE/Minorities/Females/Veterans/Disabled are encouraged to apply.