Clearance Level Needed: Secret - TS/SCI

Category: Government

Location: Washington DC Metro Area

Cyber Security Professional

The Cyber Security Professional will be responsible for working closely with the organizations project teams to ensure information system security concerns are addressed during the development of an Information System. The Cyber Security Professional will be responsible for reviewing system/application Audit Logs and support the organizations Information System Security Manager (ISSM) on all cyber related matter concerning the customers systems. The Cyber Security Professional will be responsible for preparing, implementing, and maintaining the organizations Body of Evidence (BOE) and project documentation to include the System Security Plan (SSP), Risk Management Plan, System Inventory Assessment, and Information Assurance Assessments that accurately reflects the security protection measures for each information system under the customers purview in compliance with the Community certification and accreditation process. The tasking will involve full system certification and accreditation on systems under the customers' purview. The Cyber Security Professional will provide system architecture and information assurance support on the development, integration, and operations and maintenance of Customer systems deployed on the Community infrastructure, following the project development life cycle compliance with the Community Project Management and security processes. The customer is continually searching for ways to improve our processes and provide better services to our customers. The Cyber Security Professional is expected to provide insight into better ways of doing business and support us in the effort.

Duties:

1. Ensure information system security concerns are addressed during the development of an Information system.
2. Prepare, implement and maintain the organizations Body of Evidence (BOE) to include System Security Plan (SSP), Risk Management Plan, and System Inventory Assessment.
3. Provide insight into industry trends and make recommendations on future direction for the program.
4. Utilize complex analysis tools to identify and correct problems.
5. Provide technical/analytical recommendations for improvement.
6. Work with the customer to improve metrics for reporting.

Required:

1. Demonstrated on-the-job experience in Information Security/Information Assurance/Cyber Security, specifically as related to Enterprise and operational networks and systems.
2. Demonstrated on-the-job experience showing familiarization with security vulnerability testing tools such as Nessus, AppDetective, NMAP, WebInspect, & self-scans.
3. Demonstrated on-the-job experience collaborating and working with Subject Matter Experts (SMEs) on developing authorization packages in support of achieving Authority to Operate (ATO) within required timelines.
4. On-the-job experience with compliance management using the RMF

Desired:

1. Demonstrated on-the-job experience with Cloud Computing Technologies, particularly AWS.
2. Demonstrated on-the-job experience communicating complex technical concepts and project information clearly and concisely to both technical and non-technical audiences.
3. Demonstrated on-the-job experience with a software package used for processing the A&A process.
4. Bachelor of Science and/or Masters of Science (MS) in Information Assurance/Cyber security.