INFORMATION SYSTEMS SECURITY OFFICER IN LINTHICUM HEIGHTS, MD

Job Description

Client: Enterprise Government Integrator

Location: Linthicum, MD

Compensation: Competitive based on years of relevant experience & education

Clearance: Active DOD Top Secret clearance

Description of Work:

- Designs, tests, and implements state-of-the-art secure operating systems, networks, and database products
- Conducts risk assessment and provides recommendations for application design
- Participate in a wide range of security issues including architectures, firewalls, electronic data traffic, and network access
- Uses encryption technology, penetration and vulnerability analysis of various security technologies, and information technology security research; and may prepare security reports to regulatory agencies
- Ensures systems are operated, maintained, and disposed of in accordance with internal security policies and practices outlined in the security plan
- Ensures that all users have the requisite security clearances, authorization, and need-to-know, and are aware of their security responsibilities before granting access
- Ensures configuration management (CM) for security-relevant IS software, hardware, and firmware is maintained and documented
- Ensures all information system security-related documentation is current and accessible to properly authorized individuals
- Maintains records, outlining required patches/system upgrades that have been accomplished throughout the information system's life cycle
- Ensures that all systems/network are compliant and in scope of current accreditation
- Evaluates proposed changes or additions to the information system, and advises the Information Systems Security Manager (ISSM) of their security relevance

- Create and maintain Plan of Action and Milestones (POAM) or Risk Acceptance/Acknowledgement Letters (RALS)
- Assist with security education / Conduct training sessions
- Participate in internal / external security audits/inspections
- Directs program system administrators on security matters
- Performs weekly audits as directed by the Information Systems Security Manager (ISSM)

Basic Qualifications:

- Bachelor's Degree with 5+ years of experience; or 10+ years of relevant work experience in lieu of degree. Degree must be in a Computer Sciences, Cybersecurity, Management Information Systems, or related field.
- DOD 8570 Compliant; Must have one of the following: Security+CE, CISSP, CCNA, CISM, CAP
- 3-5 years of past experience in an ISSM/ISSO role or similar joint responsibilities
- Experience with SCIF/SAPF/Secured environments
- Knowledge of NISPOM information system requirements, particularly chapter 8; MCITP/MCSA 2008/2012 & NIST/RMF/NISPOM/JAFAN/DCID 6/3 knowledge; RMF is the focus.
- ICD 503 (RMF), JSIG, and JAFAN knowledgeable
- Knowledge of and experience with Defense Security Service ODAA processes and procedures
- Windows environment experience; and the ability to develop and implement IS certification test(s) and conduct ongoing periodic reviews

Preferred Qualifications:

- Hands on experience with vulnerability scanning tools (ie. Nessus/Security Center)
- Experience/Knowledge of Splunk or other SIEM (Security Information and Event Management) products
- Knowledge of Windows security / group policy and Cisco networking
- Involvement in security audits/inspections
- Familiarity with DISA Security Implementation Guides (STIGs)
- Background of understanding of System Security Plans (SSP)

Send Resume to info@intellectualpoint.com job.