

Job Title: Information Security Analyst III (Risk Management Analyst)
Location: Fort Polk, LA
Type: Full-time
Salary: Commensurate with experience/education

Requirements:

Qualified candidates will have the following:

- Minimum of five years' experience performing Information Systems Analysis preferably as part of a government branch.
- Experience with Infrastructure as a Service (IaaS) and private/on-premise cloud infrastructure (i.e., OpenStack, NSX, vCloud, vRealize, Azure Stack, AWS Outpost).
- CCNA certification.
- IAT Level II certification.
- CompTIA Security Plus certification.
- Valid drivers license with clear record.
- Active/recent U.S. government security clearance.

Desired:

- CASP.

Job Description:

- The RMF Analyst is responsible for developing processes and procedures to communicate, report, and distribute cyber direction at the Program level to all ISSMs, ISSOs, and Information Security Owners, as well as maintain, establish, and monitor RMF transactions within the JSP Implementation Plan.
- Process/review AOR requests, and ensure compliance with all NIST, DoD, DISA, and JSP policies and procedures.
- Maintain ACAS scanning solutions on unclassified (5000+ systems) and classified networks.
- Generate reports from ACAS scanning data to assist in securing both networks.
- Use PowerShell scripting to automate tasks and create tools for the Cyber security team improving efficiency.
- Work within eMASS to support RMF auditing.
- Work using ACAS scanning data to help identify systems with vulnerabilities and work to remediate vulnerabilities.
- Write supporting documentation, logging, and reporting vulnerabilities on both networks.
- Manage the CCP access via eMASS, audit removable media, data writes, and data write authorization groups and approvals annually.
- Act in a liaison role to help assist embedded ISSO for organizational information systems throughout the Risk Management Framework (RMF) process.
- Create Project Management Plans (PMP) for systems, scheduling, and preparing Kick-Off meetings, creating and maintaining appointment orders in eMASS.
- Send escalations when timelines (based on the PMP) are not being adhered to.
- Support internal and external inspections such as the Command and Control Readiness Inspections (CCRI) performed by DISA.
- Process Removable Media Exemptions request for the user community.
- Prepare project plans and execute the implementation of RMF for assigned systems.
- Perform control validation activities, initiate the Plan of Actions & Milestones (POA&M), and compile support artifacts in eMASS.
- Monitor compliance with cyber security policy, as appropriate, and review the results of such monitoring.
- Evaluate the effectiveness of solutions implemented to provide the required protection of data, including appropriate authenticator management, encryption controls, and patch and vulnerability management processes.

Benefits:

- Medical, Dental, Vision
- Whole and Term Life Insurance
- Short- and Long-Term Disability
- Supplemental coverage (Aflac)
- 401(k)
- Paid Vacation, Sick Leave, Holidays
- Paid Bereavement and Jury Duty

Physical Requirements:

While performing the duties of this job, the employee is regularly required to:

- Talk and hear.
- Stand, walk, sit.
- Lift and move items over 25 pounds.
- Use repeated wrist and finger movements.

Clearance

Selected candidates will be subject to a government security investigation and must meet eligibility requirements for access to classified information/spaces. Hire dates are contingent upon the issuance of an interim or final government security clearance.

Background Check:

Offers are contingent upon successful completion of professional reference checks, employment verification, and background screening.

GStek, Inc. is proud to be an Affirmative Action/Equal Opportunity employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identify, national origin, disability status, protected veteran status, or any other characteristic protected by law.

GStek encourages veterans, disabled veterans and disabled individuals to apply for any open position for which they feel they are qualified.

EOE Minority/Female/Veteran/Disabled