Job Description

Job Title:	**Cyber Security Analyst [IMC0031]**		
Location:	Remote	**Travel Required:**	Minimal
Level/Salary Range:		**Position Type:**	Full-Time
Date Posted:	9 January 2019	**Posting Expires:**	When Filled
Mandatory Job Requirements:	**A VA designated High-Risk Background Investigation (BI) clearance preferred, or the ability to obtain such clearance.**		

Applications Accepted By:

E-mail: Michelle Might, Corporate Recruiter, michelle.might@imcva.com
Email Subject Line: Cyber Security Analyst [IMC0031]

Job Summary

Position Summary: Candidate will join a team tasked with providing support services to the United States Department of Veterans Affairs to ensure a secure, compliant, effective, and efficient cloud architecture is implemented by the agency. In addition, candidate will be responsible for collaborating at various levels of the organization to assist in developing definitive guidance for Agency system owners to migrate operational systems to the cloud while maintaining or achieving Authority to Operate (ATO).

Candidate will be expected to collaborate with customer staff with responsibilities for Governance, Risk, Compliance and Information Security. Understanding and influencing enterprise requirements as appropriate in order to drive GRC platform development requests, from design, configuration, system development, through service implementation and application usability in order to scale and adapt to current and emerging requirements.

Along with an excellent work ethic, strong candidates will possess the motivation to accept and accomplish tasks with minimal guidance. The ideal candidate is self-managed, flexible, and team-oriented with exceptional communication skills and an ability to proactively identify customer needs to manage risks associated with a project.

Job Duties:

Responsibilities include but are not limited to:

- Reviewing existing Agency infrastructure and security documentation, performing interviews of key personnel, and reviewing technical control implementations of agency authorized cloud environments.
- Person(s) will be required to document detailed design implementation recommendations to enable our customer to remain in compliance with federal regulations and industry best practices while identifying opportunities to increase visibility and oversight into production system operations in the cloud.
- Working with customer Network Operations Center and Security Operations Center to ensure that required data feeds and views are correlated, centralized, and provide staff with a seamless transition from traditional internal network monitoring to blended monitoring of internal networks, private cloud instances, and CSP leveraged environments.

Ideal candidate will possess and demonstrate a high-level of knowledge in the following areas:

- Securing cloud environments, including: public, private, or hybrid cloud services that meet federal guidelines and regulations and NIST Special Publication best practices (e.g. NIST SP 500-292, NIST SP 800-53 Rev. 4)
- Designing, implementing, and configuring secure cloud architecture solutions within Cloud Service Provider environments (e.g. AWS, Azure) and within customer private clouds
- Supporting project teams during system design to promote the effective deployment of IT assets to cloud environments in a secure and compliant manner
- Cloud computing infrastructure, application development methodologies, best practices, and available and emergent services in CSP environments to support these functions
- Available cloud security solutions focused on: Data Governance, Risk Management, Endpoint Security, Network Visibility and Advanced Threat Monitoring and Management
- Migration of infrastructure, data and applications out of legacy data centers into cloud environments
- Security requirements applicable to Federal agencies with health care responsibilities (e.g., HIPAA, PCI, FedRAMP, FISMA, SOX, TIC, NIST, etc.)
- Review and assess customer SIEM deployments and required data/security views monitored for internal IT assets for applicability/feasibility in cloud environments
- Developing or assessing metrics and measures to reflect and illustrate the security, effectiveness, and efficiency of leveraged cloud environments

Required skills:

- Four-year degree in Computer Science or a related technical degree (or a minimum of five years of progressive IT experience in networking or cyber security)
- **A VA designated High-Risk Background Investigation (BI) clearance preferred, or the ability to obtain such clearance.**

Knowledge of the following preferred:

- Identifying and recommending Federally compliant cloud solutions for private clouds and IaaS or PaaS CSPs.
- Document detailed designs for a Cloud infrastructure based on industry best practices in cloud computing, for an IaaS or PaaS CSP environment.
- At least one industry recognized certification (AWS, Azure, CCSP, CISSP, etc.).
- Experience with CSP log and monitoring solutions (e.g., AWS Cloud Watch, and Azure Monitor)
- Experience with secure network communication techniques and protocols.

Background Information

Innovative Management Concepts, Inc. (IMC), a Service-Disabled Veteran-Owned Small Business, provides systems engineering and information technology services to government and commercial clients. As a Service-Disabled Veteran-Owned Small Business, IMC places a special emphasis on recruiting and hiring veterans. Since its founding in 1989, IMC has offered expertise in: software development, verification, and validation; technology and project forecasting; continuous feedback and organizational communications; training systems; IT architectures; and website development, maintenance, and help desk support. Find out more about IMC at www.imcva.com. ***IMC is an Equal Opportunity Employer***