Job Description

Job Title:	**Cybersecurity Analyst Sr. - IMC0086**		
Location:	Arlington VA	**Travel Required:**	Minimal
Level/Salary Range:	Based on Qualifications	**Position Type:**	Full-Time
Date Posted:	2 Aug 2019	**Posting Expires:**	When Filled
Mandatory Job Requirements:	• **Must have IAM Level III Certification or higher.** • **Minimum of 5 years cybersecurity experience.** • **Please note that pursuant to a government contract, this specific position requires U.S. Citizenship.** • **All applicants must have current DoD Secret clearance eligibility day one and prior to entry on duty with the ability to pass an SSBI background investigation to up-scope their clearance to Top Secret/SCI.**		
Applications Accepted By:			
E-mail: Michelle Might, Corporate Recruiter, michelle.might@imcva.com **Email Subject Line**: DOIM Cybersecurity Analyst Sr.			
Job Description			

In support of the Army National Guard (ARNG) National Capital Region (NCR) Director of Information Management (DOIM) contract, the cybersecurity analyst senior will report to the cybersecurity manager and provide onsite (Arlington, VA) support to the Army National Guard Information Operations Division. The cybersecurity analyst senior will be responsible for assisting to maintain a healthy security posture for an end-user community of nearly 4,000. The cybersecurity analyst senior will work with the Cybersecurity Team to conduct security scans, evaluate security compliance, make security improvement recommendations, develop security documentation to include policies and procedures, and validate security compliance for network access requests.

Responsibilities:

- Physical, personnel, facility, information systems, through policies and controls IAW Army Regulations, Department of Defense (DoD) Directives and Instructions.
- Manage information security risks and report findings to the Government.
- Develop and maintain an OPSEC Standing Operating Procedure (SOP)/Plan. The Senior Cyber Security Analyst will become OPSEC Level II certified.
- Maintain ARNG NCR DOIM IT infrastructure in a manner compliant with Federal Information Security Management Act (FISMA), DoD Risk Management Framework (RMF) and National Institute of Standards and Technology (NIST) guidance.
- Ensure that ARNG NCR DOIM LAN and its management systems are compliant with all Information Assurance Vulnerability Alerts (IAVAs).
- Conduct weekly Assured Compliance Assessment Solution (ACAS) scans and remediate vulnerabilities according to SLA.
- Ensure appropriate Secure Technical Implementation Guidelines (STIG) are maintained.

- Review Host Based Security Solution (HBSS) and Tanium reports for end point security compliance; remediate identified vulnerabilities as required.
- Track Information Assurance Vulnerability Management (IAVM) compliance.
- Create Plans of Action & Milestones (POA&M) for identified vulnerabilities.
- Report ARNG NCR DOIM security compliance to higher level authorities and/or reporting structures.
- Maintain the Information Security Plan.
- Support and validate access requests for ARNG NCR DOIM network access and Managed services through Service Operations.
- Provide consultation on Cybersecurity perspectives for proposed changes, initiatives, and projects.
- Maintain and draft memorandums for record, system interconnection agreement, and/or equivalent to document all system connections to ARNG NCR DOIM networks.
- Validate ARNG NCR DOIM managed assets are in compliance with Army Gold Master configuration, NSA Configuration Guidance and NIST Configuration Guidance through coordination with Asset Management.

The Senior Cyber Security Analyst will support C&A activities including:

- Ensure the ARNG NCR DOIM complies with the Tenant Security Plan (TSP) for the ARNG portion of DODIN-A NIPR and SIPR in support of the ARNG Authority to Connect (ATC) and Authority to Operate (ATO).
- Test the security technical controls for the ARNG NCR DOIM LAN.
- Conduct an internal review and execute all checks and tests in accordance with RMF.
- Develop a Security Test and Evaluation (ST&E) Test Plan that addresses all the requirements identified in NIST SP 800-53 and the appropriate DoD, Army, and ARNG information system security testing requirements.

The Senior Cyber Security Analyst will support the CCRI process including:

- Ensure ARNG NCR DOIM compliance with all applicable CCRI requirements (e.g. Technical, CND Directives, Contributing Factors, etc.). Report status, findings, and results.
- Provide support to the CCRI assessment team during scheduled and unscheduled inspections.
- Track CCRI findings through POA&Ms and report status during MPSRs.
- Support post-CCRI finding remediation. Assist with the planning, execution, and documentation of CCRI finding remediation activities.

Basic Required Qualifications and Skills:

Note: These are mandatory items that all candidates must have when making application to IMC for this position. Please ensure that your submission addresses each of these requirement items. Candidates without these required elements will not be considered.

- Minimum of 5 years of cybersecurity experience.
- IAM Level III certification.
- A relevant educational degree in one of the follow fields: Computer Science, Information Systems, Information Technology, Cyber Security, Computer Engineering, Information Technology, Information Security and Assurance, or Systems Engineering.
- Demonstrate excellent oral, written, and analytical communication skills.
- Strong analytical and problem-solving abilities.

- Excellent interpersonal skills with the ability to work as part of a team.
- Self-starting with strong attention to detail.
- **Please note that pursuant to a government contract, this specific position requires U.S. Citizenship.**
- **All applicants must have current DoD Secret clearance eligibility day one and prior to entry on duty with the ability to pass an SSBI background investigation to up-scope their clearance to Top Secret/SCI.**

Desired Qualifications and Skills:

It is desirable that the candidate has the following qualifications:

- IAT Level II Certification.
- ITIL Foundation v3 Certification.
- Demonstrated experience with BMC Remedy 7.6 or 9.1.
- Proficiency in Microsoft Office products: Word, Excel, PowerPoint, SharePoint, Outlook, Visio.
- Experience working with SharePoint document libraries and lists.

Background Information:

Innovative Management Concepts, Inc. (IMC), a Service-Disabled, Veteran-Owned Small Business, provides a broad range of information technology services to government and commercial clients. Since its founding in 1989, IMC has offered solutions and expertise in: IT operations and maintenance, cyber security, systems and network engineering and support services, cloud/hosting services, software engineering and development, website services, software quality assurance and testing (including IV&V), and project management. IMC is certified in International Organization for Standardization (ISO) 9001:2015 Quality Management, ISO 27000:2013 Information Technology Security Management, and ISO 20000:2011 Information Technology Service Management. Find out more about IMC at www.imcva.com.

We are an equal opportunity employer and all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, disability, protected veteran status, or any other characteristic protected by law.