Job Description

Job Title:	**Senior Cyber Security Analyst**		
Location:	Arlington VA	**Travel Required:**	Minimal
Level/Salary Range:	$140,000 - $150,000	**Position Type:**	Full-Time
Date Posted:	30 October 2018	**Posting Expires:**	When Filled
Mandatory Job Requirements:	ITIL 2007/2011 Foundation-level Certification (Current) Information Assurance Management (IAM) or Information Assurance Technical (IAT) Level II **All applicants must be a U.S. Citizen and have current security (SSBI) clearance eligibility with full collateral investigation with sensitive compartmented information, day one and prior to entry on duty**		
Applications Accepted By:			
E-mail: Michelle Dionne, Corporate Recruiter, michelle.dionne@imcva.com Email Subject Line: Senior Cyber Security Analyst – ANG NCR DOIM			
Job Description			

The senior cyber security analyst is responsible for all areas of IT cybersecurity and in assisting the ARNG NCR DOIM in managing the risk of operating a network including the Command Cyber Readiness Inspection (CCRI) and Certification and Accreditation (C&A) support and tracking.

Responsibilities:

The senior cyber security analyst is responsible for ensuring the following aspects of Cyber Security:

- 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.

The senior cyber security analyst will

- 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.

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.

- IAM Level III Certification – one or more of the following current certifications:
  - GSLC – GIAC Security Leadership Certification
  - CISM – Certified Information Security Manager
  - CISSP – Certified Information Systems Security Professional (or Associate)
- IAT Level II Certification – one or more of the following current certifications:
  - GSEC – GIAC Security Essentials Certification
  - Security + – CompTIA Security +
  - SSCP – ISC Systems Secured Certified Practitioner
- ITIL 2007/2011 Foundation Level Certification (current).
- **All applicants must be a U.S. Citizen, and have current security (SSBI) clearance eligibility with full collateral investigation with sensitive compartmented information, day one and prior to entry on duty.**

Desired Qualifications and Skills:

- Experience managing and using the Cyber tools used at the DOIM.
- A relevant educational degree in one of the follow fields: Computer Science, Information Systems, Information Technology, Cyber Security, Statistics, Business Administration, Systems Engineering, Computation Science, Computer Engineering, Electrical Engineering, Data Analytics, Information Technology, Information Security and Assurance, Mathematics, Software Engineering, Systems Engineering, or Telecommunications.

***This position is contingent upon IMC's award of the ANG NCR DOIM IT Support Task Order now being competed under the GSA VETS 2 GWAC. ***

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. As a Service-Disabled Veteran-Owned Small Business, IMC places a special emphasis on recruiting and hiring veterans. Find out more about IMC at www.imcva.com.

IMC is an Equal Opportunity Employer