503 Wando Park Blvd, Suite 100
Mt. Pleasant, SC 29464
843.958.8900
www.modus21.com

**Position Title: Modus21 Security Specialist 3 for USMC IdOps**
Status: Permanent
Location: Charleston, S.C.

Modus21 is a Charleston, South Carolina based business and technology consulting firm specializing in solving complex business problems for global business and government clients. Our philosophy is simple – provide value to our clients through the ability to streamline, measure, and improve their business processes via business intelligence and business architecture. Our expertise has proven highly successful in helping organizations recognize greater value by aligning their strategy and objectives to technology and execution.

Modus21 has been awarded a contract to provide SPAWARSYSCEN Atlantic with a series of Software Support Activity (SSA) / System Integrator (SI) and Systems Engineering support services for the Marine Corps System Command (MCSC) Identity Operations program, which includes the following systems: Identity Dominance System –Marine Corps (IDS-MC) and Forensics Exploitation Capability (EFEC).

The Security Specialist 3 will serve as Key senior cybersecurity strategy consultant for the project and provide strategic guidance to senior leaders on cybersecurity issues. The ideal candidate will have a minimum of six (6) years' experience in relevant Information Assurance and complete knowledge of Risk Management Framework (RMF), including but not limited to Assessment and Authorization package creation, security control assessment, and IT security POA&M creation.

**Responsibilities:**
- Protect system(s) by defining access privileges, control structures, and resources.
- Recognizes problems by identifying abnormalities; reporting violations.
- Implements security improvements by assessing current situation; evaluating trends; anticipating requirements.
- Determines security violations and inefficiencies by conducting periodic audits.
- Upgrades system(s) by implementing and maintaining security controls.
- Keeps users informed by preparing performance reports; communicating system status.
- Assist and support analytical efforts regarding cybersecurity policy and strategy documents.
- Assist in the development and integration, and the continual improvement of processes associated with the cybersecurity domain.
- Interact with senior Government personnel to ensure that the required cybersecurity business solutions are sufficient, appropriate, and accurate.
- Facilitate strategic-level meetings and presentations with senior Government personnel.

**Requirements/Experience:**
- BS degree in Engineering, Network Security, Management Information Systems, Information Systems, or Computer Science
- Six (6) years of experience of hands-on experience with IA controls and IA documentation, to include at least one (1) of the following two (2) areas in support of obtaining and maintaining an authority to operate (ATO): Defense Information Assurance Accreditation and Certification Process (DIACAP) or Risk Management Framework (RMF) submittal.
- Recognized expert will possess at least one (1) of the following current (not expired) certifications: CompTIA Advanced Security Practitioner (CASP), Certified Information Systems Security Professional (CISSP), GIAC Certified Incident Handler (GCIH), Certified Information Systems Auditor (CISA), GIAC Certified Enterprise Defender (GCED), or GIAC Security Essentials Certification (GSEC).
- Must be a US citizen and hold or be able to obtain a Department of Defense (DoD) Secret Security Clearance