Our growing company is searching for experienced candidates for the position of information assurance security specialist. If you are looking for an exciting place to work, please take a look at the list of qualifications below.

Responsibilities for information assurance security specialist

- Maintain, track, and validate DISN and DIA connection approval packages, including those from USASOC, its Component Commands, and other subordinate organizations
- Assist USASOC, its Component Commands, and deployed forces with the enforcement of A&A, DoD, DIA, USASOC, Component Command, and deployed forces' connection standards for networks and systems
- Provide dedicated, on-site support for Cybersecurity policy, plans, and procedures
- Develop, publish and review Cybersecurity policy and guidance, to include SOPs, TTPs, policy memorandums, directives, instructions, manuals, Task Orders, CONOPs, COOPs, ISAs, MOAs, and MOUs
- Notify the appropriate USSOCOM, Component Command, TSOC and deployed forces' Government personnel about Cybersecurity-related incidents, threats, and other general information (e.g., fake web sites, banking and phishing scams) in a timely manner
- Manage Cybersecurity information in a way that provides ready access for rapid correlation, analysis, and dissemination
- Assist USSOCOM, its Component Commands, TSOCs, and deployed forces with collaborative Cybersecurity planning and operations
- Disseminate Cybersecurity information to decision makers, to the Computer Network Defense (CND), Network Operations (NetOps), and information operations communities, to support planning, operations, and other related

- Evaluate guidance from higher headquarters, coordinate applicable implementation by USSOCOM, its Component Commands, TSOCs and deployed forces, and draft recommended direction
- Provide dedicated, on-site support for Cybersecurity reporting

Qualifications for information assurance security specialist

- Experience with HPE ArcSight auditing appliance/function a plus
- Compile metrics and create Cybersecurity reports for CTOs, IAVM, FISMA, DoD, USCYBERCOM, NSA, DISA, and DIA compliance reporting
- Track IAVM, CTO, and Warning Order (WARNORD) Compliance
- Analyze trends and publish summary reports at least monthly
- Report metrics in support of IA compliance requirements
- Comply with the IT System Rules of Behavior and report any potential violations of the Rules of Behavior to the Government Computer Security Incident Response Team