SECURITY ENGINEER IN FORT BELVOIR, VA

The client is looking for a candidate who can perform program management functions for INSCOM and plan, coordinate, and manage activities to enable the execution of the RMF and ICD 503 for INSCOM and its 16 MSCs information systems and applications. Coordinate with INSCOM, DAO, a DoD agency, Army CIO/G6, OMB, NETCOM, MSC elements, system owners, vendors, and system developers to collect and verify information assurance (IA) artifacts, policies, and procedures and prioritize and plan RMF and ICD 503 required activities for testing and documenting security control compliance and risk mitigation. Coordinate and conduct technical vulnerability scans of INSCOM systems and applications using approved DoD and Army tools and verify and validate inherited and technical IA controls and mitigations strategies versus DoD standards. Prepare, register, and submit system information and Program of Action and Milestones (POA&Ms) to federal databases to comply with DoD and Army directives and regulations and implement and document Certificate of Networthiness (CoN) processes for INSCOM systems and applications. Coordinate and provide guidance, assistance, and recommended courses of action for system owners to ensure compliance with DoD, Army, and INSCOM Cybersecurity policies and prepare and submit executive RMF and ICD 503 packages to the AO or DAO for review and signature. Track information system assessment and authorization (A&A) status and prioritize and plan for annual security control compliance activities. Collect and verify continuity of operations (COOP) and disaster recovery (DR) plans to validate compliance with mission assurance requirements and standards and provide IA training and awareness to INSCOM and MSC system and application owners.

Basic Qualifications:

- 2+ years of experience with Cybersecurity and IA and JWICS accreditation support, DoD IA RMF, DIACAP, DCID 6/3, and ICD 503
- 2+ years of experience with developing and presenting technical information and presentations to non–technical audiences and clients
- Knowledge of DoD, Army, and intelligence community IA and security laws, regulations, and policies, including mandates
- Knowledge of FISMA and reporting requirements, including eMASS and Xacta usage
- DoD 8570
- Compliant Certification, including Security+ required

Additional Qualifications:

- Experience with JWICS C&A procedures, DIACAP, DCID 6/3, and ICD 503 processes and POA&M tracking and resolution
- Experience with DoD security technical implementation guides (STIGs) and checklists and DoD testing tools, including Gold Disk, Security Readiness Review scripts (SRRs), and SCAP and the Retina Nessus ACAS scanning tool
- Experience with DoD 8500, AR 25–2, AR 380–5, AR 380–40, DCID 6/3, ICD 503, FIPS, DoD, and Army IA policies
- Possession of excellent oral and written communication skills
- BA or BS degree
- DoD 8570–Compliant Certification, including CISSP preferred

Clearance

- Candidates must be US citizens and able to obtain and/or maintain a Department of Defense Top Secret security clearance as a condition of employment

Send Resume to careers@intellectualpoint.com