

As a **Global Mission Network (GMN) Senior Network Engineer** (Systems Engineer IV), you will provide non-personal support to the U.S. Army Network Enterprise Technology Command (NETCOM) efforts in the engineering, planning, integration, and management support to the Points of Presence (POPs), Virtual Server Stacks (VSSs), Mission Network Access Kits (MNAKs) and Global Mission Network (GMN) Black Core components and services.

Highlights of Responsibilities:

- Analyzing and resolving problems with the Global Mission Network Black Core and its multiple Secret-level networks over a common mission network infrastructure between the RHN located at Fort Bragg, Camp Roberts, Landstuhl, Kuwait, and Guam; and the Mission Network Points of Presence.
- Analyzing and resolving problems with Cisco Internet Operating system (IOS), Cisco NXOS, ASA firewalls, data packet routing, switching, proxy services, and engineering for IP data networks, VPNs, and IPSEC.
- Providing configuration, integration, and Tier III support for the terrestrial transport connecting the RHNs (regional hub nodes) and virtual data centers.
- Analyzing and resolving problems with system provisioning and network connection requirements and methods to connect a remote MNAK to CENTRIX-SWA (CX-SWA) POPs.
- Analyzing and resolving problems with Cisco validated designs for VMware vSphere 5.1 on FlexPod Data ONTAP Operating in 7-Mode Deployments.
- Analyzing and resolving problems with KG-175 and KG-250 series of NSA encryptors and management software such as GEM X and ViaSat VINE Manager, as well as with WAN acceleration technologies such as Riverbed products.
- Supporting NetOps capability integration for classified missions on mission networks such as CX-I, CX-SWA and SIPRNET networks.

Requirements:

- Current Active Secret (SSBI) Security Clearance and or the ability to obtain one, IT Level I Secret SSBI in accordance with AR 25-2.
- IAT III / IASAE II certified as specified in DOD 8570.01-M and BBP 05-PR-M-0002 (CASP, CISSP, or other specific IA Certification).
- Current Computing Environment (CE) certification (attainable within 6 months of performance start date): Cisco Certified Networking Professional (CCNP) or VMware Certified Professional - Network Virtualization (VCP6-NV)
- Bachelor's Degree in IT with 7 years of practical experience or 12 years of direct relevant technical experience.

Preferred Education and Experience:

- Hands-on experience with how Microsoft Enterprise products and tools interrelate in order to ensure NetOps capability integration in support of the classified missions on mission networks such as CX-I and SIPRNET networks. Examples of Microsoft Enterprise products and tools are Active Directory, Exchange, SCOM, SCCM, WSUS, and KMS.
- Experience in all aspects of network security and working knowledge of the following operating

systems and applications: Linux, Microsoft, Cisco Internet Operating system (IOS), Cisco NXOS, ASA firewalls, data packet routing, switching, proxy services, and engineering for IP data networks, VPNs, and IPSEC.

- Have experience in troubleshooting IP data networks using devices such as NetScout and/or WireShark.
- Working knowledge of WAN acceleration technologies such as Riverbed products. Hands-on experience with KG-175 and KG-250 series of NSA encryptors in classified and coalition networks and working knowledge of management software such as GEM X and ViaSat VINE Manager.
- Experience with and a working knowledge of SIPRNET data center operations and functions such as but not limited to IT continuity of operations and disaster recovery (COOP/DR) strategies and planning and service delivery.
- Experience in Microsoft Windows and Linux operating systems, virtual machines (VM) and stand-alone servers to include directory services, messaging, access control processes, and integrating application servers into the GMN Black Core environment.
- Experience with virtualization technologies in Operating Systems (OS), Network, Storage Area Network (SAN), and security devices.