As an **Active Directory Senior Systems Engineer**, you will provide services in support of the U.S. Army Network Enterprise Technology Command (NETCOM). You will provide operational and technical engineering support for the implementation, testing, integration, interoperability, and sustainment of information technologies comprising NETCOM Enterprise capabilities. You will support engineering support, testing and technical support in the implementation of the Network Operations (NetOps) capabilities. Support government efforts in continued deployment of enterprise NetOps capabilities that directly support the Army's maturing transformation and modularity concepts, doctrine, architecture, and organizations.

This effort provides direct support to the NETCOM CG Priorities:

1. Accomplish the Mission while always taking care of our People and Families
2. Operationalize the Command
   a. Establish clear roles/responsibilities within the Command
   b. Standardize our operational/Technical implementations and processes across the Command
   c. Build an Operational Support capability within the Headquarters
3. Integrate vertically with ARCYBER/Second Army and horizontally with our Supported Commands
4. Lead and synchronize the execution of the Army's Network Modernization effort
   a. Build on, inherently Joint network based on centralized management; decentralized execution
   b. Accelerate the Army's network collapse efforts, strategic and tactical
5. Rapidly build and employ Cyber Mission Forces and Capabilities
6. Set and then balance our team to match resources to mission across all Theaters.

Highlights of Responsibilities:

- Provides security engineering and analysis supporting the implementation of EDS&A across the AEI.
- Conducts and document security risk threat assessments, prepare recommendations for countermeasures.
- Provides security-related technical expertise for the h/w and s/w components. Also, provide processes and procedures, input determination and analysis to the security policies, risk analysis, accreditation package analysis, and engineering change proposal analysis.
- Provides security expertise to support development of Operational CM baselines for EDS&A tools and systems.
- Develops procedures, such as an implementation guide.
- Implements and standardizes Directory Service, Identity Management, and AD structures on the NIPRNET, SIPRNET, and DoDIN in the AEI in support of the Enterprise initiative.
- Supports the Enterprise AD architecture design and migration fielding. Perform NIPRNET/SIPRNET/DoDIN AD migration support to an AD and EDS environment.
- Provides operational engineering and support the establishment of the Army Enterprise AD/EDS system.
- Supports AD infrastructure design and migration.
- Identifies and provides enterprise h/w and s/w requirements for IDAM.
- Verifies and validates the Army Directory Services architecture IAW industry best business practices. Modifies network design infrastructure to identify PPS for global Enterprise constructs.
- Review and recommend alignment of project requirements with related AD applications, and

EDS enterprise designs and plans. Provide engineering integration support to mitigate unforeseen technical issues during CCRM.

- Develops standardized GPO, and IPSec model, design and management in support of the multiple AD/EDS environments across the Army, and develop programmatic scripts as necessary. Identify and confirm that derived enterprise solutions are consistent, are without redundancy, and do not negatively impact operations.
- Conducts AD and enterprise testing for related operational RFC submitted to NETCOM. Provide and document design integration of proposed technologies for the Army Enterprise.
- Provides EDS/RDS system sustainment engineering and analysis support for the legacy EDS.
- Provides input for Project RFC submissions for CMB review.
- Technical support in defining, documenting, and sustaining system internal (Army) and external (DISA) Common Interfaces (CIs) for consistent and persistent delivery of Exchange services as delivered from the DISA Defense Enterprise Computing Center (DECC) environment.

Requirements:

- Current Information Assurance (IA) certification (required at performance start date): IAT III (CASP, CISSP). IA Certification Category and Level (IAW DoD 8570.10-M and BBP 05-PR-M-0002)
- Current Computing Environment (CE) certification (attainable within 6 months of performance start date): Microsoft Solutions Associate MCSA certification
- Clearance (required at performance start date): IT Level II (in accordance with AR 25-2) SECRET T3
- Bachelor's Degree in IT with seven years practical experience or twelve years of direct relevant technical experience may be substituted for education.
- Seven years of hands-on experience with how Directory Services products and services interrelate in order to ensure NetOps capability integration in support of the LWN mission.
- Working knowledge and understanding of enterprise Directory Services concepts, AD, Messaging, and EDS procedures. The Contractor shall have expertise in all aspects of Microsoft Windows operating systems to include implementing directory services, messaging, and application servers into the enterprise environment.

Preferred Education and Experience:

- Preferred IASAE III (CISSP- ISSEP, CISSP-ISSAP)