

**Type of Requisition:** Regular

**Clearance Level Must Be Able to Obtain:**None

**Public Trust/Other Required:** None

**Job Family:** Cyber Security Technical Analysis

At GDIT, people are our differentiator. As a Senior Engineering Architecture Analyst supporting the VA Enterprise Security Architecture (ESA) Modernization Support project, you will be trusted to work actively with GDIT security and Cyber-Security professionals to support our VA customer.

Our mission within the VA is to ensure Veteran's information, VA information systems and infrastructure is cybersecurity ready. GDIT will accomplish this while ensuring the resiliency of VA's cybersecurity infrastructure through proactive monitoring, adaptive responses, adherence to Federal requirements and best practices, and the recruitment, retention, and development of a world-class cybersecurity workforce.

The ideal Enterprise Senior Engineering Architecture Analyst will have extensive experience coordinating with program and project leaders to analyze IT system and network architecture. The right candidate will have the knowledge and skill to clearly identify strategies for addressing requirements, risks, and issues and be able to effectively conduct trade-off analysis of requirements against fiscal, schedule, and performance issues. This resource is able to quickly resolve issues and create architectural vision for the ESA leadership team.

**This role is fully remote!**

#### **RESPONSIBILITIES :**

- + Supporting and providing guidance for system development and implementation planning through assessment of system engineering plans and system integration and test plans
- + Lead a team engaged in the technical design and engineering functions
- + Direct the technical organization to ensure progress according to technical objectives within budgetary and schedule guidelines
- + Oversee the design of both new and existing IT modernization, expansion, and improvement projects; analyze, evaluate, and plan methods of approach
- + Develop solutions to highly complex technical problems
- + Provide technical leadership and consulting across the organization, from strategic decision making down to the project planning level.
- + Gain organizational commitment for high-level infrastructure plans and initiate and participate in projects to evaluate technologies and methods for implementation.
- + Ensure solutions and activities delivered are aligned with the strategy and vision of the organization
- + Collaborate with fellow teammates and VA counter parts on complex architectures and recommend improvements
- + Assist in the deconstruction and interpretation of requirements supporting team projects

- + Commit to staying abreast of both emerging technologies and evolving customer goals and objectives
- + Adhere to standards, policies, protocols, procedures and best practices that truly embody a “Best of Breed” Development & Engineer services delivery team
- + Participate in architectural and design discussions as they pertain to Future State, Concepts, and planned or active Development & Engineering projects
- + Participating in strategic engagements and events, as required
- + Brief stakeholders on planned and active projects and activities

## **QUALIFICATIONS**

### **Required Skills and Experience**

- + Master’s Degree in Computer Science, Engineering, Math, or technical equivalent with at least 15 years of experience. Ten (10) years of additional relevant experience may be substituted for education
- + Demonstrated experience in Information System Security Engineering
- + Experience with security requirements in enterprise architectures including reference models, design patterns and solution architectures; and the systems supporting those missions and business processes
- + Experience with evaluating system security designs and system architectures, including network segmentation, authentication, NIST security controls
- + At least three (3) years of experience designing and developing large integrated systems
- + Ability to obtain a Public Trust clearance (T4)
- + US Citizenship is required
- + Must be able to meet customer facility COVID requirements

### **Desired Skills and Experience**

- + Possess one or more of the following certifications:
- + Microsoft Certified Systems Engineer
- + VMware Certified Professional
- + Cisco Certified Design Expert
- + AWS Solution Architect Professional
- + Azure Solutions Architect Expert
- + CISSP-ISSAP, ISSEP, CEH
- + Strong knowledge of IT Development, Engineering, Integration & Testing processes
- + Experience managing enterprise networks, network devices and cybersecurity core services

Familiarity working with VA information systems

+ Active VA clearance

+ Strong verbal and written communications skills

+ Ability to effectively plan and prioritize tasking and communicate clearly regarding technical options and trade-offs

+ Knowledge of technology integration processes

+ Ability to brief technical and non-technical audiences and communicate on security threats, vulnerabilities, and risks

---

\#GDITFedHealthJobs-ESAMS

\#ESAMS

\#VeteransAffairs

COVID-19 Vaccination: GDIT does not have a vaccination mandate applicable to all employees. To protect the health and safety of its employees and to comply with customer requirements, however, GDIT may require employees in certain positions to be fully vaccinated against COVID-19. Vaccination requirements will depend on the status of the federal contractor mandate and customer site requirements.

We are GDIT. The people supporting some of the most complex government, defense, and intelligence projects across the country. We deliver. Bringing the expertise needed to understand and advance critical missions. We transform. Shifting the ways clients invest in, integrate, and innovate technology solutions. We ensure today is safe and tomorrow is smarter. We are there. On the ground, beside our clients, in the lab, and everywhere in between. Offering the technology transformations, strategy, and mission services needed to get the job done.

GDIT is an Equal Opportunity/Affirmative Action employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, disability, or veteran status, or any other protected class.