Van Dyke Technology Group is an Information Engineering firm providing Net-Centric Security Solutions to the Intelligence Community, the Department of Defense and other Federal Agencies. We have several Security Engineer opportunities in the Columbia, MD area. Candidates must be US citizens and be willing to undergo a background investigation to obtain a government security clearance. Interested candidates should apply to: recruiting@vdtg.com.

Senior ISSE

Functions:
- Supports the Government in the design, development, implementation, and/or integration of IA architectures, systems, or system components
- Provides the Government assistance to ensure that the architecture and design of information systems are functional and secure, including program of record systems and special purpose environments with platform IT interconnectivity
- Performs system or network designs that encompass multiple enclaves, to include those with differing data protection/classification requirements
- Applies knowledge of IA policy, procedures, and workforce structure to design, develop, and implement secure networking, computing, and enclave environments

Education and Experience:
- Fourteen years of IA System Architect and Engineer (IASAE) experience, to include recent experience within the last five years, with Defense-in-Depth principles and technology, including access/control, authorization, identification and authentication, Public Key Infrastructure (PKI), network and enterprise security architecture
- Two years of experience applying security risks assessment methodology to system development, including threat model development, vulnerability assessments, and resulting security risk analysis
- A Master’s Degree in Computer Science or IT Engineering is desired and may be substituted for six years of experience
- Knowledge of Federal, NSA, IC, and DoD Information Security regulations, publications, and policy
- DoD 8570 compliance with IASAE Level 3 requirements (CISSP-ISSEP, CISSP-ISSAP)

Senior Security Controls Assessor

Functions:
- Conducts verification and validation for security compliance of all information systems, products, and components
• Analyzes design specifications, design documentation, configuration practices and procedures, and operational practices and procedures
• Provides identification of non-compliance of security requirements and possible mitigations to requirements that are not in compliance
• Conducts on-site evaluations
• Validates the security requirements of the information system
• Verifies and validates that the system meets the security requirements
• Provides vulnerability assessment of the system
• Coordinates penetration testing
• Provides a comprehensive verification and validation report (certification report) for the information system
• Provides process improvement recommendations
• Assists the Government to draft standards and guidelines for usage

Education and Experience:
• Twelve years of related work experience
• A Bachelor’s Degree in Computer Science or IT Engineering may be substituted for four years of experience
• Experience in security or system engineering in five or more areas, including: telecommunications concepts, operating systems, databases/DBMS, middleware, applications, web-servers, SANS/Netaps, Active Directory, firewalls, and controlled interfaces
• DoD 8570-1M Change 2 IAT Level III (GSE, SCNA, GCIH, CEH, CISA, CISSP) or IAM Level III requirements (GSLC, CISM, CISSP), including certification in an operating system such as Linux/Unix or Windows 7. The desired windows certification is the Microsoft Certified Information Technology Professional (MCITP).

Penetration Tester

Functions:
• Subject matter expert providing testing expertise for support of the Risk Management Framework
• Directs and/or participates in the testing phase of the security controls assessments using specialized knowledge of network protocols, operating systems, architectures, equipment, services, and standards
Education and Experience:
- Twelve years of related work experience
- A Bachelor’s Degree in Computer Science or IT Engineering may be substituted for four years of experience
- Proficient in utilizing a wide variety of tools for vulnerability and penetration testing
- Experience in performing both network and application-level testing using established test protocols and methods
- Proficient in researching and evaluating emerging technologies relevant to information systems security; interpreting agency specific and federal security regulations
- DoD 8570-1M Change 2, CEH, IAT Level III (CISA, CISSP, GSE, SCNA, GCIH, CEH) or IAM Level III requirements (GSLC, CISM, CISSP), including certification in an operating system such as Linux/Unix or Windows 2007, CCNA

**IT Security Specialist (Senior) (ISSO/ISSM)**

Function:
- Provides support for a program, organization, system, or enclave’s information assurance program
- Provides assistance for proposing, implementing, and enforcing information systems security policies, standards, and methodologies
- Provides daily oversight and direction to ISSOs

Education and Experience:
- Twelve years of related work experience in the field of security authorization is required
- A Bachelor’s Degree in Computer Science or IT Engineering is desired and may be substituted for four years of experience; substitution of work experience is at the discretion of the COR
- Experience in several of the following areas is required: knowledge of current security tools, hardware/software security implementation; different communication protocols; and encryption techniques/tools
- Familiarity with commercial security products, security authorization techniques, security incident management, and PKI and authorization services