POSITION DESCRIPTION

Title:	Senior Systems Security Engineer
Location:	Washington, DC
Schedule:	Full Time
Travel:	None
Clearance Level:	**Active Public Trust (Desired but not Required)**

Summary:

We are seeking a Senior Security Engineer to join our team of experienced hands-on engineers supporting our government client in Washington, DC. You will be providing on-site hands-on expert technical engineering services on security engineering projects and supporting and working with existing security tools and systems.

Education: Bachelor's degree or equivalent professional experience in the field of information security, computer engineering, information systems or related technical or functional discipline.

Required Experience:

- A minimum of eight (8) years of relevant hands-on engineering work experience in the area of information/cyber security engineering or operations, with an emphasis on recent, relevant hands-on experience with security tools and devices such as network firewalls, web proxy, intrusion prevention system, intrusion detection systems, vulnerability scanner, and penetration testing tools.
- Two (2) or more years of hands-on experience in designing, architecting, and implementing security controls and securing enterprise-wide systems, applications, network, and infrastructure services.
- Specialization in one of the following fields with four (4) or more years of hands-on experience:
    - Implementation of DISA, CIS, or other major security controls on Windows Based operating systems and Microsoft applications using Active Directory (including .adm & .admx files and Registry configuration), PowerShell, LGPO, and other deployment methods.
    - Implementation of DISA, CIS or other major security controls on RHEL (version 5-7) or MacOS operating systems.
    - Operating System Firewall configuration on Windows and Linux Systems
    - Secure system to system communication including but not limited to RDP, WinRM, SSH.
    - System level security protocols such as IPSec, PKI, SSL.
    - Building and administering security devices such as network firewall, web proxy, data loss prevention systems, and intrusion prevention systems.
    - Building and administering Network devices (e.g., Cisco, Juniper).

- Conducting dynamic web application security testing, both manual testing and utilizing application security tools to discover exploitable vulnerabilities.
- Conducting database security assessment and monitoring.

- Strong familiarity and experience interpreting and implementing Federal compliance standards such as NIST 800-53, FIPS, FedRAMP.

Professional Certification: Maintain at least one current professional certification. Acceptable certifications include: Any SANS GIAC Security certifications (Administration, Software, Forensics, or GSE Expert), ISC2, CISSP

Benefits:

Seneca Nation Group offers competitive compensation and a strong benefits package including comprehensive medical and dental care, matching 401K, paid time off, flexible spending accounts, commuter benefits, disability coverage, and other benefits that help provide financial protection for you and your family.

Seneca Nation Group provides equal employment opportunities to all employees and applicants without regard to race, color, religion, sex/gender, sexual orientation, national origin, age, disability, marital status, genetic information and/or predisposing genetic characteristics, victim of domestic violence status, veteran status, or other protected class status. This policy applies to all terms and conditions of employment, including, but not limited to, hiring, placement, promotion, termination, layoff, recall, transfer, leave of absence, compensation and training. The Company also prohibits retaliation against any employee who exercises his or her rights under applicable anti-discrimination laws. Notwithstanding the foregoing, the Company does give hiring preference to Seneca or Native individuals. Veterans with expertise in these areas are highly encouraged to apply.