SR. NETWORK SECURITY ENGINEER IN BETHESDA, MD

Job Description

IP is immediately seeking a **Sr. Network Security Engineer** in support of an enterprise level Government Integrator in Bethesda, MD. The qualified individual will support network security, planning, and remediation activities for a large federal agency. The right person should also have strong analytical, problem solving, and communication skills with a keen attention to detail and professional experience in analysis, planning, design, specification, implementation, integration, and management of required services & equipment.

Location: Bethesda, MD

Duration: Temp to Perm

Compensation: Competitive based on years of relevant experience & education

Clearance: Able to obtain & maintain a positions of Public Trust

Responsibilities:

- Assist with the operation, maintenance, and enhancement of network systems in a variety of tasks
- Analyze and define security requirements for Multilevel Security (MLS) issues.
- Design, develop, engineer, and implement solutions to MLS requirements.
- Lead efforts to gather and organize technical information about an organization's mission goals and needs, existing security products, and ongoing programs in the MLS arena.
- Develop security standards.
- Perform complex risk analyses including risk assessment, mitigation, and remediation planning.
- Establish and satisfy information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands.
- Support customers at the highest levels in the development and implementation of doctrine and policies.

- Apply know-how to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized security features and procedures.
- Perform analysis, design, and development of security features for system architectures.

Required Qualifications:

- Bachelor's degree and at least 10 or more years of professional experience with 5 years of experience in service provider networking and security in a federal workspace
- 3 years of experience on large networks with attention to the security and operation of systems in a 24x7 environment
- Must have experience with Cisco Identity Services Engine (ISE) and VMWare
- Experience with network access controls, particularly Cisco Network Admission Control (NAC) systems
- Must have a CCNP or equivalent certification in at least one of the following areas of specialization: Service Provider, Routing & Switching, Data Center, Security or Wireless
    - CCNA will suffice, but a CCNP will be required to obtain
- Demonstrate strong oral and written communication skills, with the ability to communicate technical topics to management and non-technical audiences, as well as interface with customers on a daily basis including, but not limited to, managers, branch chiefs, researchers, and support staff

Preferred Qualifications:

- Professional experience working at the National Institutes of Health, preferably the Center for Information Technology, or equivalent federal agency such as the National Science Foundation, National Institutes of Standards and Technology, CMS, or equivalent
- Demonstrated track record supporting highly productive project teams in the delivery of qualify services
- Additional certifications in Palo Alto, F5, and/or Cisco, especially CCIE certification, written and practical exam, in at least one of the following areas of specialization: Service Provider, Routing & Switching, Data Center, Security or Wireless

Send Resume to info@intellectualpoint.com job.