Position Announcement 17-09

NATIONAL INFORMATION TECH OPERATIONS AND APPLICATIONS DEVELOPMENT

WAN ADMINISTRATOR

Office of the Federal Public Defender
Western District of Texas (San Antonio)

THE FEDERAL PUBLIC DEFENDER, Western District of Texas is accepting applications for the position of WAN Administrator, National IT Operations and Applications Development Branch, located in San Antonio, Texas. The NITOAD branch supports the federal defender program's staffed offices in 204 locations throughout the continental United States, Alaska, Hawaii, Puerto Rico, the Virgin Islands, and Guam. The federal defender program operates under authority of the Criminal Justice Act, 18 U.S.C. § 3006A, to provide defense services in federal criminal cases and related matters by appointment from the court to individuals unable to afford counsel.

Job Requirements. To qualify for WAN Administrator, a person must be a high school graduate or equivalent and have at least three years general experience and four years specialized experience. Some higher education from an accredited college or university, preferably with a concentration in computer or management-information science or a related field, may be substituted for some of the required experience. Notwithstanding any educational substitution, specialized experience in the following areas is required:

- Must possess 3-5 years' cybersecurity experience, preferred working in and/or as an analyst to a SOC /SIRT environment;
- Strong skill sets on debugging SQL stored procedures, triggers, Views, Query Optimization Techniques & query hints;
- Effectively utilize SQL Profiler;
- Understands SQL Server Metadata views and system tables;
- Familiarity with the NIST 800 publications governing the FISMA Act;
- Experience with Splunk Searching and Reporting modules -- (Splunk ITSI and Enterprise Security App) Knowledge Objects, Administration, Dashboards, Clustering and Forwarder Management. including ingest of third- party data for rendering within the dashboard or SIEM;
- Ability to manipulate large volume of data to provide requested reports or charts;
- Preferred Certification: Splunk Certified Admin;
- Experience with Active Directory, Log management tools and Vulnerability assessment tools; and
- Employment is subject to a satisfactory background investigation, including but not limited to an FBI fingerprint check.

Experience with a public defender, law offices or court functions, policies and procedures desired. This position is classified as "high sensitive." Employment will be considered provisional pending the successful completion of an initial 10-year background investigation with updates performed every five years thereafter. Continued employment will depend upon the successful completion and favorable determinations based on investigation results. Applicants must be US citizens or be eligible to work for the federal government.

Duties.

- Responsible for technical implementation, Planning, customization, integration with big data and statistical and analytical modeling, and deploying the latest version of Splunk on a Windows or Linux environment.
- Operate and maintain all Enterprise Management functions and perform EM activities. Integrate, operate, and maintain COTS and GOTS system management tools to improve the overall operation and maintenance of production systems.
- Support system administrators in updating the configuration of system management tools to meet new/changing requirements.
- Prepare, review, and evaluate documentation, specifications, test plans, and procedures.
- Support system test programs and analyze system test results.
- Evaluate emerging technologies for inclusion into current and planned architectures.
- Secure relevant information, integrates data from different sources, and identifies possible causes of problems.
- Support operations and provide support for an enterprise on Premise security solution based on Splunk, Palo Alto, Tenable, Panorama, GSX, Solarwinds, Cisco and other common network platforms.
- Support Extract, Transform, and Load operations to retrieve content from Palo Alto, Cisco and Tenable repositories as well as existing hardware, software, system boundary inventories. Maintain and present that content within Splunk.
- Design and implement broader data integration.
- Design and build detailed Splunk reporting for internal use cases.
- Conduct appropriate analysis of threats and possible security enhancements.
- Some travel and lifting equipment up to 50 Pounds required.

Provide initial problem resolution where possible

- Generate, monitor, and track incidents through resolution
- Provide software and hardware support
- Provide expert product capabilities and input into solution design, build, and test activities and documentation.

Other duties as assigned. This position requires occasional travel.

Salary and Benefits. Starting salary will be fixed commensurate with experience and qualifications within a range from JSP-12, Step 1, to JSP-13, Step 1, and currently yielding $72,168 to $85,816 per annum. The position is in the excepted service and does not have the tenure rights of the competitive Civil Service. The position does carry regular government employment benefits including health and life insurance, retirement, and the Thrift Savings Plan. Salary is payable only by Electronic Funds Transfer (direct deposit).

How to Apply. Qualified persons may apply by forwarding a letter of interest (mentioning announcement number 17-09) and résumé to: Maureen Scott Franco, Federal Public Defender, Western District of Texas, 7550 IH-10 West, Suite 200, San Antonio, Texas 78229. (Electronic submissions will not be accepted). For applicants with disabilities, this organization provides reasonable accommodations, which are decided on a case by case basis. To request a reasonable accommodation for any part of the application or interview process, contact Personnel Administrator, Victoria Longoria (210) 472-6700. Position announced July 12, 2017, subject to the availability of funds; open until filled. *The Federal Public Defender is an equal-opportunity employer.*