THE FEDERAL PUBLIC DEFENDER, Western District of Texas is accepting applications for the position of Splunk Administrator, National IT Operations and Applications Development Branch, located in San Antonio, Texas. This is a temporary position for one year and a day, with the option to convert to a permanent position with acceptable job performance. 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 a Splunk Administrator, a person must be a high school graduate or equivalent. Candidates must have demonstrated at least 5+ years of Machine Data Management & Analytics and Splunk experience to include design, configuration, and support of Enterprise Information Systems. Some higher education from an accredited college or university (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 two or more of these areas is required:

- Experience administering Splunk on a large enterprise level;
- Experience authoring technical documentation such as Installation/Deployment Procedures;
- Experience with Splunk multisite Clustering;
- Experience with developing enterprise strategic architecture and implementation of Splunk deployments;
- Proficiency with Regular Expressions, Splunk Visualizations, SPL searches, Dashboards and Drill-downs;
- Proficiency with creating custom Splunk Add-ons for new and unique sources and source types;
- Ability to perform basic and advanced scripting tasks with Splunk to automate repeatable processes;
- Experience with various network monitoring programs, such as Splunk, Wireshark, SolarWinds;
- Strong preference for those with extensive experience in architecting, developing, deploying, configuring, and administering simple to complicated Splunk deployments; and
- Splunk training and/or certifications are preferred.

Minimum Requirements:
- Extensive experience to operate and maintain Splunk log management infrastructure and leverage knowledge on several areas including IT operations, DevOps, Analytics, Information Security, and networking;
- Knowledge of intrusion detection systems and other information security products, regulations, standards, and guidelines;
- Experience and familiarity with IT management processes and software products, networking, server, application monitoring, security patching and/or web technologies;
- Experience in interacting with customers and onboarding, configuration, and optimization in Splunk;
- Experience with using scripting languages to automate tasks and manipulate data;
• Experience working in a multi-server environment;
• Ability to multitask and solve complex technical problems; and
• High quality professional writing and verbal communication skills and abilities.

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 U.S. citizens or be eligible to work for the federal government.

Duties.
The Splunk Administrator will, configure, and deploy Splunk products and log management solutions, develop automation for security tools management, create customized search heads, and develop adhoc searches using programming and development expertise in languages such as Java, Python, Shell scripting, and/or regular expression. Additional duties include:

• Recommend, monitor, and improve NITOAD’s continual deployment infrastructure;
• Help keep key systems and servers up and operational, ensuring that all systems are securely servicing all customers;
• Provide technical leadership, coaching, and mentoring for the existing staff;
• Identify issues, collaborate with stakeholders on solutions, and provide follow-up on the implementation; and
• Analyze and adapt Splunk deployment targets to support changing needs and environments.

The applicant should also demonstrate an attention to details and the ability to maintain effective working relationships with those contacted in work. 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 $74,854 to $89,011 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 20-09) and résumé to: Maureen Scott Franco, Federal Public Defender, Western District of Texas, 7550 IH-10 West, Suite 200, San Antonio, Texas 78229. No electronic submissions will be considered unless they are submitted through Indeed.com or LinkedIn.com. This includes emails to the Defender. 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. More than one position may be filled from this announcement. Position announced December 18, 2019, subject to the availability of funds; open until filled.

The Federal Public Defender is an equal-opportunity employer.