

**Position Announcement 23-05**  
**NATIONAL INFORMATION TECH OPERATIONS AND APPLICATIONS DEVELOPMENT**  
**SPLUNK ADMINISTRATOR - REVISED**  
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 Splunk Administrator, National Information Technology Operations and Applications Development (NITOAD), 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 the position of Splunk Administrator, a candidate must be a high school graduate or equivalent and have at least three (3) years general experience and two (2) 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. The candidate must also possess strong analytical skills to solve complex technical problems, and the ability to understand and identify areas for continual development. Be detail-oriented and motivated to find opportunities to increase adoption; be available to participate in installation and maintenance activities during nights and weekends; and be available to work on-site in San Antonio, Texas. Applicants must have demonstrated proficiency in:

- (a) identifying data correlations and patterns, creating visualizations and custom reports;
- (b) working with customers to process data from multiple sources;
- (c) preparing configurations, data enrichment, and optimizations to a SIEM;
- (d) using scripting languages to automate tasks and manipulate data;
- (e) providing excellent customer service through both oral and written communication;
- (f) working with peers to create effective team collaboration.

The ability to lift 50 pounds and occasional travel, including overnight travel, is required. The selected candidate must successfully complete a ten-year background investigation with periodic updates every five years thereafter. Employment will be considered provisional pending the successful completion of the initial ten-year background investigation. Continued employment will depend upon the successful completion and favorable determinations based on investigation results thereafter. Applicants must be US citizens or be authorized to be employed by the federal government. Employment also requires a person be fully vaccinated for COVID-19 and provide proof of such prior to entrance on duty.

**Duties:** The Splunk Administrator will design, configure, deploy, and maintain Splunk and other log management systems. Regular responsibilities include providing technical coaching and mentoring to staff, identifying opportunities to increase Splunk adoption, identifying new use cases, and maintaining efficient log processing solutions. Identifying problem areas and finding solutions to collaborate with SMEs of other technology domains. Analyzing data sources and ensuring the logs processed are CIM compliant. Manipulating searches and correlations to increase processing efficiency. Creating custom searches and dashboards for non-technical customers. Performing data analysis to identify correlations, create data models, and look up tables and transforms. Maintaining the Splunk environment patches and upgrading to the recommended version. Maintaining Splunk add-ons and collaborating with diverse teams in developing custom log searches, scheduled and ad-hoc alerts. Work well as part of a team; nurture and maintain a good working relationship with peers and customers. The full position qualifications statement with position description is available upon request.

**Selection Criteria:** The successful applicant will have a minimum of two (2) years of experience administering a SIEM in an enterprise environment, authoring technical documentation such as installation, deployment, and maintenance procedures, designing, planning, and implementing complex SIEM architectures. The applicant must possess hands-on experience maintaining complex enterprise-level logging systems fully hosted on Windows Servers; have proficiency creating Regular Expressions, Visualizations, complex searches, Dashboards and Drilldowns, the ability to adapt add-ons or plug-ins for new and unique log sources and source types; demonstrate the skills to build scripted tasks to automate repeatable processes; and administer log sources equivalent to Windows universal forwarders, event logs, Syslog-NG, heavyforwarders, search clusters, and Sysmon log sources. Valid SIEM training certificates for advanced power users' education is preferred. Splunk certifications are strongly preferred. Knowledge in the administration and maintenance of datasources in a Windows environment is desirable. Proficient with PowerShell and Python 3 is strongly preferred.

**Salary and Benefits.** The starting salary will be commensurate with the experience and qualifications of the applicant within a range of \$63,736 (JSP-9, Step 1) to \$99,764 (JSP-13, Step 1) per annum. The position is in the excepted service and does not have the tenure rights of the competitive Civil Service. The position does offer federal government employment benefits, including health and life insurance programs, retirement, and the Thrift Savings Plan. Salary is payable only by Electronic Funds Transfer (direct deposit).

**How to Apply.** You may submit your application via Dice.com, USAjobs.gov, or via email to [NITOAD\\_Admin@fd.org](mailto:NITOAD_Admin@fd.org). Qualified persons may apply by submitting a letter of interest addressed to Maureen Scott Franco, Federal Public Defender, Western District of Texas, 7550 IH-10 West, Suite 200, San Antonio, Texas 78229, please reference announcement number 23-05, include a resume and a list of three professional references. Emails sent directly to the Defender will not be considered. For applicants with disabilities, this organization provides reasonable accommodations, which are determined on a case-by-case basis. To request a reasonable accommodation for any part of the application or interview process, contact personnel administrator Victoria B. Longoria at (210) 981-2081. Position originally announced November 1, 2022, and modified April 06, 2023, subject to the availability of funds; open until filled.

*The Federal Public Defender is an equal-opportunity employer.*