

**Position Announcement 21-09**  
**NATIONAL INFORMATION TECH OPERATIONS AND APPLICATIONS DEVELOPMENT**  
**WAN ADMINISTRATOR (TEMPORARY/PERMANENT)**  
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. 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 Network Administrator, a person must be a high school graduate or equivalent and have at least demonstrated 5+ years of network design and architecture experience, to include LAN, WAN, and production datacenter environments supporting web-hosting components and infrastructure, including web servers, application servers, load balancers, mail and DNS servers; 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 two or more of the following areas is required:

- Installing, maintaining, configuring and troubleshooting a variety of LAN/WAN equipment, including routers, switches, load balancers and security appliances;
- Solid knowledge in routing technologies included but not limited to BGP, MPLS OSPFv2/v3, EIGRP for IPv4/IPv6 and RIPv2;
- Implementing and supporting enterprise Wi-Fi deployments;
- Working with various network monitoring programs, such as Splunk, Wireshark, and SolarWinds;
- Operating, administering and maintaining experience with RADIUS, TACACS+, DMPVN and VPN technologies;
- Understanding of firewalls, load-balancing, switches and routers;
- Understanding of Splunk especially feeding syslog and other data into Splunk (servers, workstations and NetFlow data from applications like Palo Alto, SolarWinds, Cisco etc); and
- Implementing and supporting IP video conferencing systems.

This position is classified as "highly 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.** The network administrator provides consultation, day-to-day network administration, and support to the defender network with a strong customer-oriented focus in providing technology services. Assists in developing, monitoring, and deploying the national Federal Defender security technology programs. Responsible for the maintenance of equipment configurations, technical support for all issues related to network systems, planning and development of new infrastructures, expansion of existing services, and security to protect the network infrastructure and equipment at the data centers. Specialized duties include maintaining and resolving issues in routing, switching, VoIP, video conferencing and security incidents, and analyzing intrusion detection data. If ticket escalation to vendors on provided hardware and software solutions are necessary, the following specialized duties are required:

- Responsible for technical implementation, planning, customization, integration with big data and statistical and analytical modeling;
- Provide expert product capabilities and input into solution design, build, system installation; defining, documenting, and enforcing system standards;

- Establish networking environment by designing system configuration;
- Read and analyze bandwidth logs and utilization reports;
- Operate and maintain all Enterprise Management functions and perform EM activities. Integrate, operate, and maintain Commercial off-the-shelf (COTS) and Government off-the-shelf (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 investigate data from different sources and identify possible causes of problems;
- Support vendor managed VoIP services in conjunction with Vendor;
- Serve as an escalation point between customers and vendor managed services 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;
- Provide initial problem resolution where possible;
- Generate, monitor, and track incidents through resolution;
- Provide software and hardware support;
- Serve as a Level 3 technical support to other IT professionals;
- Some travel and lifting equipment up to 50 Pounds required; and
- Other duties as assigned.

The applicant should also demonstrate an attention to detail and the ability to maintain effective working relationships with those contacted during the course of work.

**Salary and Benefits.** Starting salary will be fixed commensurate with experience and qualifications within a range from JSP-9, Step 1 to JSP-13, Step 1, and currently yielding \$59,908 to \$92,795 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 21-09) and résumé to: Maureen Scott Franco, Federal Public Defender, Western District of Texas, 7550 IH-10 West, Suite 200, San Antonio, Texas 78229 or you may submit your letter of interest and resume in a single PDF document by email to [NITOAD\\_Admin@fd.org](mailto:NITOAD_Admin@fd.org). The document should be named as follows: "Announcement number, position title, last name, first name" (e.g. 21-09 WAN, Smith, John). Electronic submission may also be through Indeed.com or LinkedIn.com. Electronic submissions to the Defender 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 at (210) 981-2081. More than one position may be filled from this announcement. Position announced February 6, 2021 subject to the availability of funds; open until filled.

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