



VACANCY ANNOUNCEMENT

United States Bankruptcy Court for the Western District of Virginia

VACANCY # 2019-02

POSITION: IT Security Officer/Network Administrator

POSTING DATE: October 22, 2019

TYPE: Full-Time

Duty Station: Roanoke, VA

SALARY RANGE: \$49,772 - \$80,933 (CL 27)*

*Starting salary dependent upon qualifications and experience. Promotion potential to CL 28 without further competition.

CLOSING DATE: Position will remain open until filled, with priority given to applications received by November 12, 2019.

Check the status of this position at www.vawb.uscourts.gov/employment-opportunities

POSITION OVERVIEW

The United States Bankruptcy Court for the Western District of Virginia is accepting applications for a full-time, permanent IT Security Officer/Network Administrator. The IT Security Officer/Network Administrator performs work related to the implementation and administration of information technology security policies and practices, collaborates with other regional and national judiciary stakeholders on security-related matters, and provides network administration for the court, to include day-to-day operational support for the court's IT infrastructure, help desk support for end users, and installation/configuration/troubleshooting of hardware and software systems. The position requires the incumbent to be proactive and able to analyze IT security problems and assess the practical implications of alternative solutions. It also requires excellent communication skills and the ability to translate technical terms into non-technical language.

REPRESENTATIVE DUTIES

- Conducts security risk and vulnerability assessments of planned and installed information systems to identify weaknesses, risks, and protection requirements. Utilizes standard reporting templates, automated security tools, and cross-functional teams to facilitate security assessments.
- Provides security analysis of IT activities to ensure that appropriate security measures are in place and are enforced.
- Reviews, evaluates, and makes recommendations on the agency's IT security programs, including automation, telecommunications, and other technology utilized by the court.
- Assists with the development and maintenance of local court unit security policies and procedures, the remediation of identified risks, and the implementation of security measures to ensure information systems' reliability and to prevent and defend against unauthorized access to systems, networks, and data.
- Develops, analyzes, and evaluates new and innovative information technology concepts, approaches, methodologies, techniques, services, guidance, and policies that will constructively transform the information

- security posture of the court. Makes recommendations regarding best practices.
- Oversees the implementation of security on information systems and the generation of security documentation for system authorization and operation. Manages information security projects (or security-related aspect of other IT projects) to ensure milestones are completed in the appropriate order, in a timely manner, and according to schedule.
 - Coordinates the court's response to SOC Alerts, virus alerts, and handles remediation.
 - Provides hands-on installation, configuration, and deployment of court computing systems and mobile devices; develops software deployment packages; provides end-user training on hardware/software as needed; provides input and recommendations regarding IT-related projects; and manage large IT projects as assigned.
 - Monitors and responds to day-to-day Help Desk activity, logs computer problems, and troubleshoots and repairs system issues. Provides information and assistance to end users on applications and software. Maintains high satisfaction (both internal and external) through successful and timely resolution of technical problems.
 - Creates user accounts and automated forms and customizes programs for local needs.
 - Manages Active Directory, Window Server devices, VOIP NIPT phone systems, and the production of virtual environments (VMware, vSphere servers, View Desktops, and COOP environment).
 - Manages Distributed File System (DFS) and DFS Replication; installs, configures, and monitors Cisco devices (Switches, Firewalls, ISE, Wireless LAN Controllers, and Wireless Access Points); monitors system and network performance and system vulnerabilities; and manages servers, Storage Area Network (SAN), and BIOS/Firmware upgrade. Provides day-to-day systems backups and verifies the validity of data.
 - Creates and documents all actions, practices, procedures, and processes and submits regular status updates and reports to the Systems Manager.
 - Performs other duties as assigned.

MINIMUM QUALIFICATIONS

- High school graduate or equivalent with at least two years of specialized IT security and network administration experience equivalent to CL-25 or higher.
- Strong understanding of IT security best practices and demonstrated ability to analyze, design, implement and train security procedures.
- In-depth knowledge of IT, software, networks, and theories, principles, practices, and techniques of data communications and network management, traffic, and security.
- Ability to consistently demonstrate sound ethics and judgment and to work well with others
- Excellent interpersonal and communication skills (written and verbal) and ability to clearly explain technical terms and processes in non-technical language.
- Ability to coordinate and manage diverse technical support tasks and multiple competing projects while adhering to stringent deadlines.

PREFERRED QUALIFICATIONS

- A Bachelor's Degree in computer science or related field from an accredited four-year college or university.
- CISSP, CISM, or similar certification.
- Experience with Nessus Vulnerability Scanner, Splunk Log Management, Symantec Endpoint Protection, Malwarebytes, KACE Patch Management, ForcePoint Web Protection, AirWatchMDM, Palo Alto firewalls, WebSense.
- Experience with JAVA, Linux, and SQL server programming and administration.

CONDITIONS OF EMPLOYMENT

- Applicants must be United States citizens or eligible to work in the United States.
- This is a high-sensitive level position within the Federal Judiciary. The selected candidate will be hired provisionally, pending the successful completion of the required background investigation and favorable employment suitability determination. Reinvestigations will be required every five years thereafter.

- Employees must adhere to the Code of Conduct for Judicial Employees which is available at: www.uscourts.gov/rules-policies/judiciary-policies/ethics-policies
- Judiciary employees are considered “at will” employees and can be terminated with or without cause.
- Electronic Funds Transfer (EFT) for payroll deposit is required.
- Occasional travel both within the district and outside the district will be required.

BENEFITS

The Federal Judiciary offers a number of exceptional benefits including paid annual and sick leave, 10 paid holidays per year, health and life insurance, vision and dental insurance, a flexible benefits program, participation in the Thrift Savings Plan (similar to a 401K plan, with employer matching), long-term care insurance, and participation in the Federal Employees Retirement System. Additional information on benefit programs can be found at www.uscourts.gov/careers/benefits.

APPLICATION PROCEDURES

Email the following list of required application documents to vawb_careers@vawb.uscourts.gov and reference Vacancy #2019-02 in the subject line. Documents must be submitted in a **single PDF file** in the following order:

1. Cover letter:

- Reference job vacancy number # **2019-02** and include an email address in your contact information

2. Chronological resume which includes:

- Education, work history, names and addresses of current and prior employers, dates of employment, work performed, significant accomplishments, three to five references

3. Application for Judicial Branch Federal Employment (Form AO 78) available at:

www.uscourts.gov/forms/AO078.pdf

- All sections of the application must be completed. Description of Work sections must list pertinent information. Do not type “see resume”.
- After completing the form, please ensure the content you provided is saved properly and the form is not blank when you submit with your application documents.

The United States Bankruptcy Court for the Western District of Virginia is an Equal Opportunity Employer