



U. S. District Court  
Southern District of Mississippi

NETWORK ADMINISTRATOR  
Vacancy Announcement MSSD-2019-03

**POSITION**

Network Administrator

**LOCATION**

Jackson, Mississippi

**SALARY/TARGET**

CPS 27/28 (actual salary dependent on relevant experience and qualifications)

The entry level salary range is \$49,772 through \$74,596

**POSITION AVAILABLE**

July 8, 2019

**APPLICATION  
CLOSING DATE**

Open Until Filled.

**ANNOUNCEMENT**

MSSD-2019-03

The U. S. District Court, Southern District of Mississippi, is an Equal Opportunity Employer

**POSITION OVERVIEW / RESPONSIBILITIES**

**The United States District Court for the Southern District of Mississippi is accepting applications from qualified applicants for the position of Network Administrator. This position is located in the Clerk's Office at the Thad Cochran Courthouse in Jackson, Mississippi.**

The Network Administrator will have responsibility for monitoring network infrastructure and components, implementing upgrades and improvements, designing and deploying work stations, servers and software; additionally the incumbent will assist the Director of Information Technology (IT Security Officer - ITSO) in performing professional work related to the management of information technology security policy, planning, development, implementation, training, and support for the court unit. The incumbent aids the ITSO in fulfilling security objectives within the court.

**REPRESENTATIVE DUTIES**

- Analyze needs, coordinate, and configure computer network systems to increase compatibility and share information. Train other technicians to work with computer systems and programs. Diagnose hardware and software problems and replace defective components. Maintain and administer computer networks and related computing environments, including computer hardware, systems software, and all configurations. Recommend changes to improve systems and configurations, as well as determine hardware or software requirements related to such changes. Maintain network security.
- Analyze, develop, and implement short-term and long-range automation improvement plans for the court, ensuring that the changes can be implemented with minimal disruption at the court site.
- Plan for disaster recovery operations and testing, including network performance, security, anti-virus, intrusion, web usage/monitoring, design, and acquisition of servers. Produce useful system documentation, perform system startup and shutdown procedures, and maintain control records.

- Monitor network infrastructure and components, including all servers and workstations, and implement improvements to performance and security. Design, modify, enhance, test and implement standard configurations for deployment of network components and associated software packages.
- Evaluate, recommend, and implement processes to improve efficiencies and performance of the networks through the development or purchase of products to automate and monitor routine tasks such as server and workstation maintenance activities, performance monitoring and reporting, installation of software or firmware upgrades, patches, etc.
- Plan, coordinate, implement and test network security measures in order to protect data, software, and hardware. Identify and assess risks by performing security analysis and assist in producing detailed security plans. Oversee configuration and monitoring of firewall operations.
- Provide security analysis of IT activities to ensure that appropriate security measures are in place and enforced.
- Supervise on-site vendors. Participate in district-wide network projects. Assist with preparations for propose automation funding needs for fiscal budget.
- Lead project teams in managing information technology projects and implementing and integrating systems with other networks.
- Assist with reviewing and evaluating recommendations on the court's technology security program, including automation, telecommunications, and other technology utilized by the court. Assist with promotion and support security services available throughout the local court unit.
- Provide security analysis of IT activities to ensure that appropriate security measures are in place and are enforced. Conduct security risk and vulnerability assessments of planned and installed information systems to identify weaknesses, risks, and protection requirements. Utilize standard reporting templates, automated security tools, and cross-functional teams to facilitate security assessments.
- Assist with the identification, implementation, and documentation of security safeguards on information systems. Assist with information security projects (or security-related aspects of other IT projects) to ensure milestones are completed in the appropriate order, in a timely manner, and according to schedule. Prepare justifications for budget requests. Prepare special management reports for the court unit, as needed.
- Serve as a liaison with court stake holders to integrate security into the system development lifecycle. Educate project stakeholders about security concepts and create supporting methodologies and templates to meet security requirements and controls.
- Recommend changes to ensure information systems' reliability and to prevent and defend against unauthorized access to systems, networks, and data.
- Assist with the creation and employment of methodologies, templates, guidelines, checklists, procedures, and other documents to establish repeatable processes across the courts' information technology security services.
- Assist with establishing mechanisms to promote awareness and adoption of security best practices.
- Perform other related duties or special projects, as assigned.

## **EDUCATION AND QUALIFICATIONS**

High School diploma required; a bachelor's degree or higher from an accredited institution, in an IT or IT-related major preferred. Certified Information Systems Security Professional (CISSP), Certified Information Security Management (CISM), CompTIA Security+, CompTIA Network+ or similar certification preferred. At least five years of professional IT experience preferred.

Additionally, applicants must possess good judgment, be dependable, be a proactive self-starter, and demonstrate initiative in problem solving. The position requires exceptional ability to effectively communicate, articulate, and relate to coworkers and staff with professionalism and integrity.

Candidates must also possess the ability to exercise mature judgment, possess high ethical standards, a positive work attitude, and the ability to work harmoniously with others in a team-oriented environment. Prospective candidates must be available for overnight travel and the ability to work nights and weekends as needed. Lifting of equipment for placement is sometimes required.

## **PREFERRED TECHNICAL QUALIFICATIONS**

Knowledge or familiarization with Cisco switching and integrated wireless technologies, inner workings of computers/laptops/tablets, Microsoft Windows Server (2012 and above), Microsoft Windows Active Directory with server administration (including Group Policy administration), Microsoft Windows 10 Desktop Operating System, Microsoft Office 365 Suite, virtualization hosting software (VMWare), VoIP telephones (Cisco or similar), SAN storage systems (NetApp, Nimble or similar), Symantec Endpoint Protection, Malwarebytes Management Server, Forcepoint/WebSense, Splunk, KACE, Nessus Vulnerability Scanning and Symantec BackupExec.

## **MISCELLANEOUS INFORMATION**

- Employees of the federal judiciary serve under “Excepted Appointments” and are considered “at-will” employees and can be terminated with or without cause at any time with the exception of Probation Officers, who must be removed for cause per 18 U.S.C. 362.
- Employees of the judiciary are required to use direct deposit for their salary payments.
- Candidates must be citizens of the United States of America or be eligible to work in the United States.

## **BENEFITS**

The judiciary offers a generous benefits package which includes:

- 10 paid holidays
- Paid sick and annual leave
- Medical insurance options (requires employee contribution)
- Life insurance options (requires employee contribution)
- Retirement options including participation in the Thrift Saving Plans (tax deferred or Roth retirement savings)
- Long term care plan options
- Long term disability plan options
- Flexible spending account options

## APPLICATION PROCESS

Qualified applicants should submit the following documents:

- A cover letter and resume of qualifications, education and employment experience, including references;
- A completed Application for Judicial Branch Employment (AO 78), which is available at <http://www.uscourts.gov/uscourts/FormsAndFees/Forms/AO078.pdf>.

Applications may be submitted via email, hand delivery or mail, as follows:

**via email to:**

[hr\\_manager@mssd.uscourts.gov](mailto:hr_manager@mssd.uscourts.gov)

(subject: Network Administrator – MSSD-2019-03)

**Please note:** When submitting via email, documents should be submitted as a single PDF document.

**By mail or hand-delivery to:**

Arthur Johnston, Clerk  
U.S. District Court, Southern District of Mississippi  
501 E. Court St., Suite 2.500  
Jackson, Mississippi 39201

**MARK ENVELOPE CONFIDENTIAL**

Applications will be accepted until position is filled.

The Court reserves the right to modify the conditions of this job announcement, to withdraw the announcement, or to fill the position sooner than the closing date without prior notice.