United States District Court
Northern District of West Virginia
Vacancy Announcement

Position Title:	IT Security Administrator
Location:	Northern District of West Virginia
Opening Date:	February 26, 2026
Starting Salary:	CL 28/1 – CL 28/61 ($71,583--$133,178) Starting salary dependent upon experience, qualifications, and duty station.
Closing Date:	Open until filled. First cut-off date for review of applications is March 20, 2026.
Announcement #	WVN 2026-05

The United States District Court is seeking qualified applicants for the position of a full-time IT Security Administrator for the Northern District of West Virginia. The position will be based at one of the four points of holding court in Clarksburg, Elkins, Martinsburg, or Wheeling, and will support staff at all locations. This position may require travel within the United States.

Position Description:

The IT Security Administrator performs professional work related to the management of information technology security policy, planning, development, implementation, training, and support for their court unit. The incumbent provides actionable advice to improve IT security and fulfill security objectives within the court. The incumbent ensures the confidentiality, integrity, and availability of systems, networks, and data across the system development life cycle (SDLC), and creates, promotes, and adheres to standardized, repeatable processes for the delivery of security services. The IT Security Administrator pro-actively engages all users in security awareness and training activities to promote the appropriate use of best security practices within the court. The incumbent is responsible for implementing local security policies, processes, and technologies that are consistent with the national Information Security program as well as for collaborating with other judiciary stake holders, such as the Administrative Office and other court IT personnel, to identify and collectively advance security initiatives both within and beyond court unit boundaries.

Duties include, but are not limited to, the following:

- Review, evaluate, and make recommendations on the court's technology security program, including automation, telecommunications, and other technology utilized by the court. Promote and support security services available throughout the local court unit.
- Provide technical advisory services to securely design, implement, maintain, or modify information technology systems and networks that are critical to the operation and success of the local court unit. Perform research to identify potential vulnerabilities in, and threats to, existing and proposed technologies, and notify the appropriate managers/personnel of the risk potential.

- Provide advice on matters of IT security, including security strategy and implementation, to judges, court unit executives, and other senior court unit staff.
- Assist in the development and maintenance of local court unit security policies and guidance, the remediation of identified risks, and the implementation of security measures.
- Develop, analyze, and evaluate new and innovative information technology policies that will constructively transform the information security posture of the court unit. Make recommendations regarding best practices and implement changes in policy.
- 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. Manage 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.
- Create and employ methodologies, templates, guidelines, checklists, procedures, and other documents to establish repeatable processes across the courts' information technology security services.
- Establish mechanisms to promote awareness and adoption of security best practices
- Perform other duties as assigned.

Qualifications and Requirements: Interested applicants should have a high school diploma and five years of progressively responsible IT security experience with thorough knowledge of IT security best practices, network management and security, IT networks, network traffic, computer hardware and software, data communications, security architecture, security policies and procedures, anti-malware and endpoint security controls.

The ideal candidate will possess excellent interpersonal and communication skills (written and verbal), organization and problem-solving skills and have the ability to train and clearly explain technical terms and processes in non-technical language.

Preferred Qualifications: The following qualifications and requirements are not required, but preferred qualifications for this position:

- Prior Federal Court IT knowledge or experience.
- CISSP, CISM, or similar certification.
- Experience with vulnerability scanners, log mangers, endpoint protection, patch management, Mobile Device Manager (MDM), firewalls and switch configurations.

Miscellaneous:

- U.S. citizenship required.
- Electronic Fund Transfer (EFT) for payroll deposit is required.
- The selected candidate will be subject to an OPM background investigation that includes an FBI fingerprint check as a condition of employment.
- Employees of the U.S. District Court are "At Will" employees and are required to adhere to a Code of Conduct of Judicial Employees, which is available to candidates for review on our website at www.wvnd.uscourts.gov/
- Position will require travel.

Benefits:

Benefits include paid vacation, sick leave, paid holidays, health insurance, a flexible benefits program, a retirement plan and portable savings plan with matching contributions, and a professional environment. Additional benefit information is available at www.uscourts.gov/careers/benefits.

Application Procedure:

Qualified applicants must submit one PDF file with a completed Application for Judicial Branch Federal Employment (AO 78), a cover letter and a resume with salary history and professional references. The PDF file should be sent to:

Kelly Fry, HR Administrator
U.S. District Court
1125 Chapline Street
P.O. Box 471
Wheeling WV 26003 or kelly_fry@wvnd.uscourts.gov

U.S. District Court is an Equal Opportunity Employer