VACANCY ANNOUNCEMENT 2018-9

OFFICE OF THE CLERK
UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE

DATE:	December 11, 2018
POSITION TITLE:	IT Security Officer (Full-Time Permanent)
LOCATION:	Greeneville, TN
SALARY:	CL 27/1 to CL 28/61 ($48,951 to $95,388) – Starting salary is usually in the low to middle portion of the range provided above, depending on qualifications and experience in accordance with the Court Personnel System.
PROMOTION POTENTIAL:	There is promotion potential to the CL 28 level without competition (when determined qualified and depending upon budget).
CLOSING DATE:	December 26, 2018

POSITION OVERVIEW:

The U.S. District Court Clerk's Office for the Eastern District of Tennessee is recruiting for an IT Security Officer position responsible for IT security policy, planning, development, implementation, training, and support for the court. The IT Security Officer 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 at multiple court locations within the district. Job duties include:

- Reviewing, evaluating, and making recommendations on the court's technology security program, including automation, telecommunications, and other technology utilized by the court. Promoting and supporting security services available throughout the court.
- Providing 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 court. Performing research to identify potential vulnerabilities in, and threats to, existing and proposed technologies, and notifying the appropriate managers/personnel of the risk potential.
- Providing advice on matters of IT security, including security strategy and implementation, to judges, court unit executives, and other senior court staff.
- Assisting in the development and maintenance of court security policies and guidance, the remediation of identified risks, and the implementation of security measures.
- Developing, analyzing, and evaluating new and innovative information technology policies that will constructively transform the information security posture of the court. Making recommendations regarding best practices and implement changes in policy.
- Providing security analysis of IT activities to ensure that appropriate security measures are in place and are enforced. Conducting security risk and vulnerability assessments of planned and installed information systems to identify weaknesses, risks, and protection requirements. Utilizing standard reporting templates, automated security tools, and cross-functional teams to facilitate security assessments.
- Assisting with the identification, implementation, and documentation of security safeguards on information systems.
- Serving as a liaison with court stake holders to integrate security into the system development lifecycle. Educating project stakeholders about security concepts, and creating supporting methodologies and templates to meet security requirements and controls.
- Recommending changes to ensure information systems' reliability and to prevent and defend against

unauthorized access to systems, networks, and data.
- Creating and employing methodologies, templates, guidelines, checklists, procedures, and other documents to establish repeatable processes across the courts' information technology security services.
- Establishing mechanisms to promote awareness and adoption of security best practices.
- Acting as a technical expert in solving system problems. Providing in-person troubleshooting assistance with non-routine or more complicated issues.
- Performing tasks, including installing, troubleshooting, repairing, and configuring hardware and software.
- Assisting with office and chambers moves, reconnecting equipment in new locations.
- Assisting local users with general troubleshooting.
- Performing other duties as assigned.

GENERAL QUALIFICATIONS:

- Exceptional organizational and time management skills. Ability to handle multiple tasks simultaneously.
- Excellent interpersonal skills. Ability to maintain a professional demeanor, exercise mature judgment and to be a dependable and flexible team participant.
- Excellent written and oral communication skills with the ability to explain technical concepts in an understandable manner. Proficiency at writing effective instructions for users and fellow staff.
- Ability to independently analyze, isolate, and solve problems in complex systems.

MINIMUM EXPERIENCE AND/OR EDUCATION REQUIREMENTS:

A relevant associate degree and a minimum of two years of specialized experience defined as: progressively responsible information technology experience related to the management of IT security policy, planning, development, implementation, training, and support.

Classification level will be set based on the work experience, qualifications, and salary history of the successful candidate.

To qualify at a CL 27**,** at least one year of the required specialized experience must be equivalent to work at the CL 25. Completion of a bachelor's degree from an accredited college or university AND one of the following superior academic achievement requirements can be substituted for the minimum experience requirements:

- An overall "B" grade point average equaling 2.90 or better of a possible 4.0;
- Standing in the upper third of the class;
- "3.5" average or better in a major that involves information technology; or
- Completion of one academic year (18 semester or 27 quarter hours) of graduate study in an accredited university in a field closely related to the subject matter of the position.

To qualify at a CL 28, at least one year of the required specialized experience must be equivalent to work at the CL 27. Completion of a Master's degree or two years of graduate study (27 semester or 54 quarter hours) in an accredited university in a field closely related to the subject matter of the position can be substituted for the minimum experience requirements.

COURT PREFERRED SKILLS/QUALIFICATIONS:

- One year of specialized experience in IT security or closely related field
- A relevant bachelor's degree
- Proficiency with Nessus Vulnerability Scanner
- Experience with KACE Patch Management and SPLUNK Log Management
- Skill in documenting procedures and organizing assessment results/remediations
- Proficiency in Microsoft Windows environments and general computer networking
- Proficiency with MS Group Policy
- Knowledge of Websense/Forcepoint or similar filtering web proxy and Symantec Endpoint Protection

CONDITIONS OF EMPLOYMENT:

- U.S. District Court employees serve under "Excepted Appointments" and are considered "at will." Employment can be terminated with or without cause by the court. Federal Civil Service classifications and regulations do not apply.
- U.S. District Court employees are required to adhere to the *Code of Conduct for Judicial Employees* and are subject to strict confidentiality requirements.
- Salary payments are subject to mandatory electronic funds transfer (direct deposit).
- Applicants must be U.S. citizens or eligible to work in the United States.

BENEFITS:

Court employees are entitled to the same benefits as other federal employees such as:

- Thirteen days of paid vacation for the first three calendar years, twenty days after three years, and twenty-six days after fifteen years.
- Ten paid federal holidays per calendar year.
- Participation in a Federal Employees Health Benefits Program and the Federal Employees Dental and Vision Program.
- Participation in Group Life Insurance, Long-Term Care Insurance, and Long-Term Disability programs.
- Participation in a pre-tax Flexible Benefits Spending Account.
- Participation in the Federal Employees Retirement System with investment opportunities through the Thrift Savings Plan.

APPLICATION PROCESS:

Submit one document in PDF format via e-mail to jobs@tned.uscourts.gov that includes the following:

- A cover letter addressing the qualifications, skills, and experience necessary to perform the job;
- A resume, including a list of professional references; and
- A completed AO 78, Application for Federal Judicial Branch Employment (available on the court's website at http://www.tned.uscourts.gov/sites/tned/files/ao78.pdf).

INCOMPLETE SUBMISSIONS AND SUBMISSIONS THAT ARE NOT RECEIVED IN A SINGLE PDF FILE MAY NOT BE CONSIDERED.

- Only applicants selected for an interview will be notified.
- Applicants interviewed will take a computer skills test.
- Employment references will be checked prior to a job offer.
- The successful candidate will undergo a mandatory FBI fingerprint check/background investigation and will be considered a provisional employee pending successful completion of the investigation.
- Interviews are expected to take place in the Knoxville office. The court is not authorized to reimburse candidates for travel in connection with an interview or pay for any relocation expenses.

The Court reserves the right to modify the conditions of this job announcement or to withdraw the announcement without written notice to applicants. If a subsequent vacancy of the same position becomes available within a reasonable time of the original announcement, the Court may elect to select a candidate from the original qualified applicant pool.

THE UNITED STATES DISTRICT COURT IS AN EQUAL OPPORTUNITY EMPLOYER AND VALUES DIVERSITY IN THE WORKPLACE