CAREER OPPORTUNITY

U.S. District Court
Western District of Wisconsin

Position:	IT Security Officer
Vacancy Number:	20-02
Location:	Madison or Eau Claire, Wisconsin
Salary:	CL 28 ($59,660-$96,999) based on qualifications
Date Posted:	December 4, 2019
Closing Date:	Open until filled. Preference given to applications received prior to January 13, 2020

Position Summary

The Western District of Wisconsin is seeking a talented IT Security Officer to serve the Bankruptcy and District Courts as well as the Probation and Pretrial Services office. The successful applicant's office may be located in either Madison or Eau Claire Wisconsin. We are looking for an IT professional who loves to pro-actively advance security priorities and engage customers in security awareness, training and best practices. This position will report administratively to the District Court Chief Deputy. The district is looking for a self-starter who will improve the district's security posture and collaborate with other regional and national judiciary stake holders. As part of several information technology teams, you will work in a professional work environment to deliver impactful security initiatives for the judiciary and have the opportunity to support nationwide programs. Secondary responsibilities include assisting the network administrators in the administration of the judiciary's information technology network by developing standards, recommending network infrastructure change and participating in the high-level and long-term design and analysis of the courts' network systems as it relates to IT security.

Summary of Representative Duties and Responsibilities

- Review, evaluate, and make recommendations on courts' technology security programs. Create and employ procedures, templates, guidelines, and other documents to establish repeatable processes across the district's information technology security services.
- Proactively track, triage, and remediate identified security risks and implement security measures. Coordinate the remediation of larger security risks with other IT team members and advise management when additional resources are needed.
- Perform research to identify potential vulnerabilities in, and threats to, existing and proposed technologies, and notify the appropriate managers/personnel of the risk potential. Conduct security risk and vulnerability assessments. Perform routine scans and remediations to system vulnerabilities and monitor for outdated applications and security-related matters.
- Communicate and provide advice on matters of IT security, including security strategy and implementation to judges, court unit executives, and other court staff managers.

- Assist in the development and maintenance of local court unit security policies and guidance. Serve as a resource to all court units within the district regarding federal and judiciary security regulations and procedures.
- Manage information security projects (or security-related aspects of other IT projects) to ensure milestones are completed in the appropriate order, promptly, and according to schedule. Facilitate project meetings. Prepare justifications for budget requests. Prepare special management reports as needed.
- Establish mechanisms to promote security. Train court staff on security awareness and adoption of security best practices.
- Serve as a team lead in the administration of IT security-related automated tools, including but not limited to antivirus products, operating system/software patch management mechanisms, web security/filtering platforms, system logging facilities, and locally installed firewall appliances.
- Assist with special projects as directed by management and perform other IT support duties as assigned.
- Act as the primary contact for external security assessments and audits, and address relevant issues found.
- Perform analysis, remediation, forensics, and any other activities need concerning any IT security incidents.

Qualifications

- To qualify at the CL 28 level, the applicant must have a minimum two years of relevant security experience, including at least one year equivalent to work at the next lower level (CL 27).
- Experience with IT security tools and the ability to learn new tools and methods.
- System administration experience.
- Ability to perform independent research and identify training needs.
- Ability to collaborate with individuals, teams of any size, and organizations of any size.
- The ability to work with other local and remote technical staff to identify, prioritize, and resolve security issues - especially those identified in security scans.
- Good judgment, be dependable, be a proactive self-starter, and demonstrate initiative in problem-solving.
- Exceptional ability to effectively communicate, articulate, and relate to co-workers and others with professionalism and integrity.

Preferred Qualifications

- Experience with IT security tools used by the US Courts (Splunk, Nessus, KACE, and Forcepoint).
- Ability to create and maintain policies, end-user documentation, and instructions.
- Ability to perform internal IT security assessments and self-audits, and monitor policy adherence.

Benefits

Federal benefits include paid vacation and sick leave, paid holidays, and retirement benefits. Optional benefits include health and life insurance, disability and long-term care insurance, dental and vision insurance, and a tax-deferred savings plan. This position is subject to mandatory electronic fund transfer (direct deposit) participation for payment of net pay.

Procedures for Applying
In order to be considered for this position, go to:

https://opportunities.ilnb.uscourts.gov/Employment/appform.cfm?ref=cr92kf7g&pos=20-02

Complete the information fields and attach:

1. Cover letter that describes your interest in pursuing this position and how your experience relates to the stated duties, responsibilities, and skills and abilities of this position;
2. Judicial Branch Federal Employment Application (AO78). The AO78 is included in the link;
3. Resume with references (with phone numbers);
4. References;
5. A short (no more than one page) narrative describing your philosophy on security policy and how you keep abreast of changes.

Incomplete application packets will not be considered.

Please note:
The court is not authorized to reimburse candidates for travel in connection with an interview or to pay relocation expenses to the successful candidate.

As a condition of employment, the selected candidate must complete a background check investigation, including an FBI fingerprint check. All court employees are *at will*, and therefore the selected candidate may be removed from this position at any time if the selected candidate fails to perform at a satisfactory level. In addition, employees are required to adhere to the Code of Conduct for Judicial Employees.

The court reserves the right to modify the conditions of this job announcement or to withdraw the job announcement, or to fill the position sooner than the closing date, any of which action may occur without any prior written notice. Only applicants who are interviewed in person will receive a written response regarding their application.

Where appropriate and necessary, the court provides reasonable accommodation to applicants with disabilities.

The United States District Court is an Equal Opportunity Employer