

**UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF NEW YORK  
POSITION VACANCY 16-12  
Position Re-advertised - Original Vacancy 16-08**

**POSITION** Cyber Security Analyst

**LOCATION** Buffalo, New York

**DEADLINE** January 13, 2017, or until filled

**SALARY** CL 29 (\$69,286 – \$112,643) based on qualifications and experience

***Position Overview***

The United States District Court, Bankruptcy Court, and Probation Office for the Western District of New York are seeking qualified applicants for a full-time Information Technology Security Officer. The IT Security Officer performs professional work related to the management of information technology security policy, planning, development, implementation, training, and support for all court units within the district. The incumbent provides actionable advice to improve IT security and serves as a team lead to fulfill security objectives within the district. 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 Officer collaborates with the AO Office of IT Security to assist with the implementation and creation of national security policies and the promotion of the Judiciary Information Technology Security Program while also working with the district's court units to collectively establish and raise the security baseline of the Judiciary. 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 stakeholders to establish, coordinate, and advance security priorities across all court units within the district.

***Duties and Responsibilities***

- Review, evaluate, and make recommendations on courts' technology security programs, including automation, telecommunications, and other technology utilized by the court units throughout the district. Promote and support security services available throughout the district.
- 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 all court units. 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, unit executives, and other senior court staff. Serve as an information security resource to all court units regarding federal and judiciary security regulations and procedures.
- 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 concepts, approaches, methodologies, techniques, services, guidance, and policies that will constructively transform the information security posture of all court units within the circuit. 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.
- Oversee the implementation of security on information systems and the generation of security documentation for system authorization and operation. 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, as needed.

- Serve as a liaison with court stakeholders to integrate security into the system development lifecycle. Facilitate project meetings, educate project stakeholders about security concepts, and create supporting methodologies and templates to meet security requirements and controls.
- Assist court units in developing policies and procedures 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 district's information technology security services.
- Establish mechanisms to promote awareness and adoption of security best practices.

***Education and Experience Qualifications***

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+, or similar certification preferred. At least five years of professional IT security experience preferred, including:

- Thorough knowledge of network management and security, network traffic analysis, computer hardware and software, and data communications.
- Understanding of applicable programming languages, such as Python, Java, PHP, and SQL.
- Provides risk assessment and recommends risk mitigation strategies where appropriate.
- Designs security awareness training programs for users and IT staff applying industry standards. Creates materials and presentations; maintains training records; and coordinates and provides IT security training.
- Ability to identify and analyze security risks and to implement resolutions.
- Knowledge of anti-virus, anti-malware, application control, web threat protection and endpoint security controls. Knowledge of IPSec and the ability to use it to protect data, voice, and video traffic.
- Understanding of incident response, including the ability to implement a plan and procedures.
- Ability to work with and influence multiple court locations within the district in order to align court units' strategies with secure, high-performance systems.
- Skill in interpersonal communications, including the ability to use tact and diplomacy in dealing effectively with all levels of management, staff, and judicial officers.
- Skill in project management, organizing information, managing time and multiple work assignments effectively, including prioritizing and meeting tight deadlines.

***Benefits***

Job security, excellent benefits, good federal employee pay, and an exceptional retirement system are just a few of the reasons to consider a position with the Judiciary. In addition, a career with the Judiciary offers desirable travel opportunities, training availability, and diverse occupational opportunities.

According to the United States Bureau of Economic Analysis, the average annual salary for full-time federal government jobs now exceeds \$81,258 and the average annual federal workers compensation, including pay plus benefits, now exceeds \$123,049 compared to just \$61,051 for the private sector.

Benefits include: health, life, dental, vision, and long term care options; Federal Employees Retirement System (defined benefit retirement); matching, tax-deferred and/or Roth Thrift Savings Plan (defined contribution participation in optional Transit Subsidy Program).

***Applicant Information***

Discuss two of the biggest challenges facing IT security, and what in your opinion, can be done to reduce the threat. Discuss the primary reason most organizations have not fixed their vulnerabilities and what approach can be taken to help correct that? Review the practices identified below. Choose two practices which you feel are most important in the role of IT Security and submit a statement addressing your skills and abilities in these areas.

- |                      |                                 |                     |
|----------------------|---------------------------------|---------------------|
| • User Training      | • Policy Creation & Enforcement | • Documentation     |
| • Scanning & Testing | • Programming & Scripting       | • Incident Response |

In addition to the above statement, applicants must submit a detailed résumé, AO78 Application for Judicial Branch Federal Employment (available at [www.uscourts.gov](http://www.uscourts.gov) ), and a cover letter to: United States Courthouse, Room 200, Attention: Vacancy 16-12, 2 Niagara Square, Buffalo, New York 14202. Only candidates selected for an interview will be notified. Unsuccessful candidates will not receive notice.

### *Conditions of Employment*

- Applicants must be a U.S. citizen or a lawful permanent resident of the United States currently seeking citizenship or intending to become a citizen immediately following meeting the eligibility requirements.
- Incumbent will be hired provisionally pending the results of a background investigation and subject to updated background reinvestigations every five years.
- The selected applicant must satisfactorily complete a one year probationary period.
- Incumbent is subject to electronic deposit of salary payment.
- Positions within the U.S. Courts are “excepted service.” Employees are “at will.”
- No travel or relocation expenses permitted.
- Incumbent must adhere to the Code of Conduct available on the court’s website at [www.nywd.uscourts.gov](http://www.nywd.uscourts.gov).
- The court provides reasonable accommodations to applicants with disabilities.
- The U.S. District Court for the Western District of New York is an Equal Opportunity Employer.