United States Court of Federal Claims

717 Madison Place NW
Washington, DC 20005

POSITION VACANCY

Announcement Number:	**CFC-2018-01-IT**
Position Title:	**Computer Specialist (Security)**
Open Date:	**January 10, 2018**
Close Date:	**February 16, 2018**
Type of Appointment / Position:	**Permanent / High Sensitive**
Grade / Salary Range:	**CL-28 ($65,238 – $106,012)**
Duty Location:	**Washington, DC** (conveniently located across from the White House and Lafayette Park, one block from McPherson Square Metro)
Who May Apply:	**U.S. Citizens (or persons eligible to work in the United States)**

Position Overview and Representative Duties:

The Computer Specialist performs professional work related to the management of information technology security policy, planning, development, implementation, training, and support for the U.S. Court of Federal Claims. The incumbent provides actionable advice to improve IT security and serves as a team lead to 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 incumbent develops, deploys, and monitors IT security related systems and applications. Experience with Nessus Vulnerability Scanner, Symantec Endpoint Protection, Malwarebytes, Solarwinds, Triton Websense, Splunk, and similar systems is highly desired. The Computer Specialist 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 (AO) and other court IT personnel, to identify and collectively advance security initiatives both within and beyond USCFC boundaries.

No relocation expenses will be paid.

General Experience:

The candidate selected for this position must have investigative analytic skills to successfully perform the following duties, which include, but are not limited to:

- 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.
- Develop and deliver IT security related training and training materials for all court staff or specific groups or departments as needed; maintains blogs and/ or newsletters for the purpose of IT security familiarization and training.

- 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.
- Identify both technical and process improvements to elevate the quality of work performed by other technical staff.
- Provide statistical reports and supporting data in response to ad-hoc requests for information. This is performed in addition to routine situational awareness reporting.
- Ensure all security notifications are tracked to closure and that escalations occur consistently in accordance with documented procedures.
- Developing and maintaining processes and procedures used to manage operations and incident response processes.
- Other duties as assigned.

The successful candidate must be a self-starter as well as detail-oriented. The candidate must also be highly organized and tactful, possess good judgment, poise and initiative, and maintain a professional appearance and demeanor at all times. The candidate must have strong prioritizing and problem-solving skills, solid communication skills (written & oral) and be able to communicate effectively with clients within and outside the court. A demonstrated ability to work harmoniously with others in a team environment and to exhibit a professional manner at all times is essential.

Required Qualifications:

To qualify at the CL 28 level, the successful candidate must have at least two year equivalent specialized experience equivalent to the CL-27 level.

Preferred Qualifications:

The court requires the candidate to have a Bachelor's degree in Computer Science or a related field. Five (5) years of specialized experience which demonstrates working knowledge, skills, and abilities to successfully perform the duties of the Computer Specialist (Security)may be substituted for the degree requirement.

Benefits:

10 holidays • 13-26 days annual leave (increases with service) • 13 days sick leave • Federal Employees Retirement System • Thrift Savings Plan • Commuter Benefit Program/Metro Transit Subsidy Program • Flexible Spending Accounts • Insurance available for health, dental, vision, life, and long-term care.

How to Apply:

Ensure that your application package contains the following required documents:

- **Cover Letter** (include the Announcement Number and the position title and address your qualifications relating to the duties and responsibilities of this position);
- **Résumé**;
- **Form AO78 Federal Judiciary Application Form** which can be found at: www.uscourts.gov/uscourts/FormsAndFees/Forms/AO078.pdf;
- **Three (3) business/professional references** with name, affiliation, and contact information;
- **Salary History** for prior three (3) years;
- If a current Federal Civilian Employee, your **latest Personnel Evaluation** and your **latest SF-50**; and,
- If a current or recently discharged or retired military member, your **latest Officer Evaluation Report (OER), Enlisted Evaluation Report (EER) or equivalent, and a copy of your DD Form 214.**

***All documents must be combined in a single PDF file and e-mailed to* uscfcjobs@cfc.uscourts.gov. Zip files and faxes will not be accepted. Please include the Title and Job Announcement Number in the subject line.**

What to Expect Next

- The court will conduct an evaluation of each applicant's qualifications and materials after receipt of a complete application package.

- Applicants selected for an interview will be contacted. Interviews may commence immediately.

- The court reserves the right to modify the conditions of this job announcement, to withdraw the job announcement, and/or to commence interviews immediately, any of which actions may occur without prior written or other notice.

- This is an "Excepted Appointment" and an "At Will" position. Federal Government Civil Service classifications or regulations do not apply.

- All appointments are subject to a full background check including an FBI Fingerprint Background Check, as well as periodic reinvestigation.

- If offered employment, such employment shall be provisional pending our receipt of the results of a mandatory Fingerprint and Background Investigation. Until the background investigation is satisfactorily completed, we may only hire you provisionally. The provisional nature of your hiring, however, will not affect your start date, salary, or other benefits.

- No phone calls please. Only those candidates selected for interview will be contacted.

- The United States Court of Federal Claims is an Equal Opportunity Employer.