

UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT



POSITION VACANCY ANNOUNCEMENT

ANNOUNCEMENT NO.

CAFC-09-01

OPEN:

February 17, 2009

CLOSE:

Open Until Filled

**POSITION TITLE, GRADE
AND SALARY:**

**Information Technology Support Specialist (Security)
CL 28 (\$58,476–\$95,037)
Temporary One Year + One Day
In accordance with current recruitment, promotion
and/or demotion policies
Some Benefits Apply (Health, Life, TSP)**

LOCATION OF POSITION:

**United States Court of Appeals
for the Federal Circuit
717 Madison Place, N.W.
Washington, D.C. 20439**

POSITION OVERVIEW:

The Information Technology Support Specialist is located in the Information Technology Office (ITO) of the United States Court of Appeals for the Federal Circuit. The position is responsible for ensuring that an appropriate level of operational security is maintained for the court's information systems and programs. This involves maintaining confidentiality and integrity of the systems, networks, and data through enhancement of security assessments to identify vulnerabilities, risks, and protection needs. The position participates in network and systems design to ensure implementation of appropriate systems security policies.

Duties may occasionally require working non-business hours. The ideal candidate will have substantial experience in security configurations and controls and how they affect overall network security and performance.

REPRESENTATIVE DUTIES:

Analyzes and develops guidelines and policies for security risk analysis, security management, and audits, and performs penetration testing, vulnerability assessments, remediation, and intrusion detection of firewalls, routers, performance monitoring software, servers, and microprocessors.

Creates Disaster Recovery Plan and other related security plans.

Identifies standards for change management and controls the change process by reviewing configuration change requests. Develops information systems security plans and procedures, and ensures that they comply with federal laws, regulations, policies, and standards.

Ensures the confidentiality, integrity, and availability of systems, networks, and data through the planning, analysis, development, implementation, maintenance, and enhancement of information systems security programs, policies, procedures, and tools.

Evaluates, acquires, configures, and uses software intended to ensure that automated systems are secure from unauthorized use, viral infection, and other problems that would compromise sensitive information in terms of confidentiality, integrity, and availability, or would compromise other aspects of overall system security.

Identifies and analyzes malfunctions of resources to assist in preparing security incident reports.

Develops procedures to locate and remove software obtained from unauthorized or questionable sources.

Applies well-defined security policies and procedures to the network infrastructure.

Manages system back-ups and upgrades and, monitors system performance.

Monitors network security operations and access lists.

Performs information assurance assessments on designated systems.

Prepares information assurance documentation related to certification and accreditation of systems.

Analyzes information assurance requirements against budget, time and other mission related constraints to give a best course of action and recommendation.

Researches alternatives and performs alternative analyses.

Performs risk analysis to determine the best risk management value for the court.

Develops system security plans, contingency plans, configuration management plans, incident response plans, and security assessment reports.

Identifies and recommends technical solutions to meet specific program needs and/or enhance the IT infrastructure.

Recommends and reviews component IT procurements to assure that they can be integrated into the IT environment.

Ensures that systems support personnel correctly install and use approved security features and tools.

Ensures continuing systems security testing, and documents the results, i.e., tests user passwords, conducts security threat analyses, and tests accounts.

Manages and develops risk management plans for the court.

Performs risk assessments and analyzes vulnerabilities; documents results and prepares appropriate countermeasures.

Conducts other inspections periodically.

EDUCATION/GENERAL EXPERIENCE:

Bachelor's Degree from an accredited four-year college or university in an Information Technology, Computer Science, or related field.

Progressively responsible experience which provided an opportunity to gain: (1) a good understanding of the methods and technical skills required to accomplish the work (2) the ability to analyze problems and assess the practical implications of alternate solutions; (3) the ability to communicate with others, both orally and in writing; and (4) the capacity to employ the knowledge, skills, and abilities in the resolution of problems/issues.

If qualifying based on education, applicant's major field of study must have been in information security, computer science, information technology, information systems management, or similar course work that provided equivalent knowledge to a major in the computer field.

SPECIALIZED EXPERIENCE:

Three years of specialized professional experience including at least one year of experience equivalent to work at the CL 27 level.

Specialized experience is experience that demonstrated accomplishment of computer project assignments that required a wide range of knowledge of computer requirements and techniques pertinent to the position. This knowledge is generally demonstrated by assignments where the applicant analyzed a number of alternative approaches in the process of advising management concerning major aspects of system design, such as what system interrelationships must be considered, or what operating mode, system software and/or equipment configuration is not appropriate for a given project.

SUBSTITUTION:

Additional specialized experience may be substituted for the degree requirement on a year for year basis, up to four years.

APPLICATION PROCESS AND INFORMATION:

Mail, fax, or email a cover letter, resume and/or AO-78 (*Application for Federal Judiciary Employment-see court's website at www.cafc.uscourts.gov-click on Employment*) to:

U.S. Court of Appeals for the Federal Circuit
717 Madison Place, N.W., ASO/HR-Suite 410
Washington, D.C. 20439
Attention: IT Support Specialist CAFC-09-01
Fax to: (202) 633-5885 E-Mail: cafcjobs@cafc.uscourts.gov

(Job posting also at www.usajobs.gov)

OTHER INFORMATION:

Only qualified applicants who submit complete application packages will be considered for this position. Only those applicants selected for an interview will be contacted and must travel at their own expense. Reimbursement for travel and/or relocation is not available.

The court reserves the right to modify the conditions of this announcement, commence interviews immediately, withdraw the announcement, or fill the position at any time, any of which actions may occur without notice. No phone calls please.

NOTES: (1) If selected you may be required to complete an initial performance evaluation period of employment. Failure to successfully complete the evaluation period may result in termination of employment. (2) This is an “**Excepted Appointment**” and “**At Will**” position. Federal Government Civil Service classifications or regulations do not apply. (3) As a condition of employment, applicants must successfully complete an FBI Fingerprint and Background Check. (4) This position is subject to EFT (direct deposit of earnings). (5) Must be a U. S. citizen or eligible to work in the United States.

The United States Court of Appeals for the Federal Circuit is an Equal Employment Opportunity employer.