

UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT



POSITION VACANCY ANNOUNCEMENT

<u>Vacancy #:</u>	CAFC 23-06
<u>Posting Dates:</u>	Open until filled
<u>Position Title:</u>	IT Security Specialist
<u>Grade/Salary:</u>	CL 26 – CL 28 (\$57,222 - \$122,483) Salary determined by qualifications and experience as outlined below. Promotion up to CL 29 may occur without further posting or competition.
<u>Position Location:</u>	U.S. Court of Appeals for the Federal Circuit 717 Madison Place NW, Washington, DC 20439 Position is on-site with telework opportunities per Court policy.

About the Court

The United States Court of Appeals for the Federal Circuit (CAFC) is unique among the thirteen Circuit Courts of Appeal. It has nationwide jurisdiction in a variety of subject areas, including international trade, government contracts, patents, trademarks, certain money claims against the United States government, federal personnel, veterans' benefits, and public safety officers' benefits claims. For additional information about our court please [visit our public website](#).

Position Overview

The Information Technology Security Specialist position is in the Information Technology Office (ITO) and reports directly to the Circuit Information Security Officer. The incumbent provides security advice and technical support to operational ITO teams; develops, tests, and maintains secure system configurations; and participates in audit activities. Incumbent must demonstrate strong technical capabilities and written communication skills.

Responsibilities include, but are not limited to:

- Security Implementation – Review documented security baselines and assess the configuration on pre-production systems in the environment. Revise configuration as a result of testing and document the final recommendation for implementation. Research best practices for current systems and tools and provide recommendations to improve security and function of these tools. Engage with system owners to prioritize any improvements and communicate these recommendations to ITO management. Implement data classification, conditional data protection, and data loss prevention technologies appropriate to data sensitivity levels and in coordination with impacted user base and ITO management. Provide direct technical support to operational ITO staff to support routine activities and major projects, as needed. This includes

direct troubleshooting alongside ITO Help Desk and Infrastructure staff, configuring systems and devices prior to deployment or issuance, and replacing hardware.

- **Monitoring and Auditing** – Perform vulnerability assessments with automated tools on various system types throughout the system lifecycle. Manage remediation activities with operational ITO staff and external stakeholders. Establish and maintain logging, auditing, monitoring, and alerting capabilities of systems on premises and in cloud environments. Participate in incident response and remediation activities.
- **Planning and Assessment** – Maintain knowledge of current and upcoming security capabilities as they relate to the local environment. Test and evaluate solutions to fill identified capabilities gaps. Provide recommendations during planning for system renewal/replacement. Participate in self-assessment activities, including review of and revision to policies, plans, and process documents. Identify solutions and strategies to address underperforming areas; coordinate and participate in the implementation of these solutions and strategies.
- **General Responsibilities** – Communicate and respond to judges, chambers staff, and management requests regarding circuit operations. Communicate clearly and effectively, both orally and in writing, to explain complex operational matters and concepts to individuals and groups with varying experience and backgrounds. Interact effectively with the public and staff, providing good customer and quality service and resolving difficulties efficiently while complying with regulations, rules, and procedures. Develop, implement, and maintain written procedures for assigned functions. Comply with the *Guide to Judiciary Policy*, applicable Administrative Office policies and procedures, internal controls guidelines, and all local policies and procedures. Abide by the *Code of Conduct for Judicial Employees* and court confidentiality requirements. Always demonstrate sound ethics and good judgment. Display a careful and deliberate approach in handling confidential information in a variety of contexts.

Required Qualifications

- **CL 26 (\$57,222 - \$92,995):** Possession of a high school diploma (or equivalency) and a minimum of one year of specialized experience equivalent to the CL 25 **OR** a bachelor's degree in a closely related field from an accredited college.
- **CL 27 (\$62,852 - \$102,201):** Possession of a high school diploma (or equivalency) and a minimum of two years of specialized experience. At least one of the two years must have been equivalent to the CL 26.
- **CL 28 (\$75,343 - \$122,483):** Possession of a high school diploma (or equivalency) and a minimum of four years of specialized experience. At least one of the four years must have been equivalent to the CL 27.

Specialized experience is progressively responsible technical experience directly related to the duties and responsibilities of the position. Examples may include IT systems administration, engineering, networking, etc., with a focus on security.

Required Competencies

- Excellent teamwork and collaboration skills.
- The ability to use tact and diplomacy when interacting with stakeholders at all levels.
- Strong technical skills and a demonstrated expertise in troubleshooting complex issues.
- The ability to exercise innovative and creative skills to solve challenging issues.
- Excellent communication (both oral and written) and organizational skills.
- The ability to prioritize, manage multiple tasks, and work effectively under pressure, as well as the ability to work both independently and in a team environment.

Preferred Qualifications

- CISSP or Associate certification, or the ability to receive certification within one year from date of appointment.
- Experience securing data in a cloud environment, including classification, selective protection and DLP.
- Experience working in the information technology field for the federal judiciary.

Application Process

To be considered application packages must include:

1. Cover letter of no more than two pages, wherein the applicant describes the required knowledge, skills, abilities, and/or experience that would make them well qualified to fill this position.
2. Resume outlining educational background, employment history, and other relevant information.
3. Completion of the online AO-78, Federal Judicial Branch Application for Employment.
4. Completion of the online cognitive and customer service test.

Once you have the cover letter and résumé (items 1 and 2 above) readily accessible in PDF format, follow the below link to submit your files and complete the online AO-78 and online tests (items 3 and 4 above): <https://www.ondemandassessment.com/link/index/JP-M5VW90XA4?u=116354>

Applicants who require an exception to the online application may contact Human Resources to request an alternate method using the following email: hr@cafc.uscourts.gov.

Benefits Information

A generous benefits package is available to full-time permanent court employees including:

- Paid vacation and sick leave, paid parental leave, and 11 paid federal holidays per year.
- Optional participation in Federal Employees Health Benefits plans (health, dental and vision); Federal Employees Group Life Insurance; Flexible Benefits Program; Long-Term Care Insurance; Health Care Reimbursement (HCRA) and Dependent Care Reimbursement (HCRA).
- Public transportation subsidy, on-site fitness center, Employee Assistance Program (EAP).
- Participation in the Federal Employees Retirement System (FERS). Optional participation in Thrift Savings Plan (up to 5% employer matched contributions).
- Public Service Loan Forgiveness program pursuant to the term of the ([PSLF](#)) program.
- For more benefit information visit the [Judiciary's Benefits Page](#).

Additional Information

Only those applicants selected for an interview will be contacted and must travel at their own expense if an on-site interview is necessary. 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.

This position is on-site in Washington, DC with telework opportunities per the Court's guidelines. This is an Excepted Appointment and At Will position. Federal government civil service classifications or regulations do not apply. As a condition of employment, applicants must successfully complete an FBI fingerprint and background check. This position is subject to EFT (direct deposit of earnings).

Must be a U.S. citizen or eligible to work in the United States. Non-citizens may be interviewed and considered for employment, but employment offers will only be made to individuals who qualify under one of the exceptions in 8 U.S.C. § 1324b(a)(3)(B). Under 8 U.S.C. § 1324b(a)(3)(B), a lawful permanent resident seeking citizenship may not apply for citizenship until he or she has been a permanent resident for at least five years (three years if seeking naturalization as a spouse of a citizen), at which point he

or she must apply for citizenship within six months of becoming eligible and must complete the process within two years of applying (unless there is a delay caused by the processors of the application). Non-citizens who have not been permanent residents for five years will be required to execute an affidavit that they intend to apply for citizenship when they become eligible to do so.

The U.S. Court of Appeals for the Federal Circuit is an Equal Opportunity Employer.