UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

POSITION VACANCY ANNOUNCEMENT

Vacancy #:	CAFC-26-02-REVISED
Closing Date:	Open until filled
Position Title:	Information Technology Security Officer
Grade/Salary:	CL 26 – CL 28 ($62,212 - $133,178) Promotion up to the CL 29 may occur without further posting or competition. Salary determined by qualifications and experience as outlined below under "Required Qualifications".
Position Location:	U.S. Court of Appeals for the Federal Circuit 717 Madison Place, NW, Washington, DC 20439

****Application packages submitted for the original CAFC-26-02 Information Technology Security Officer posting will automatically be considered. If additional information is required, applicants will be contacted directly.****

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 (IT) Security Officer is located in the Information Technology Office (ITO) and is supervised by the Assistant Circuit Executive for Information Technology. The position maintains the operational security posture for the United States Court of Appeals for the Federal Circuit, performing professional work related to security policy implementation, risk assessment, vulnerability management, compliance monitoring, incident coordination, and security awareness. The incumbent collaborates with the Administrative Office IT Security Office to implement national security policies and works as a member of the ITO management team, coordinating initiatives with ITO managers and obtaining appropriate review and approval before implementing policy changes. The position coordinates with the Circuit Executive's Office on risk management matters and serves as the court's primary IT security resource.

Representative duties are intended to illustrate the major duties and responsibilities that are performed by this position. Representative duties may be adjusted, and additional duties may be added, based on the operational needs of the court and ITO. Primary responsibilities are project and program management (approximately 40-45% of time) and systems management support, compliance monitoring, and documentation (approximately 35-40% of time), with business analysis and other duties (approximately 15-20% of time) prioritized based on organizational needs and capacity.

- **Security Operations and Compliance:** Implement and maintain local security policies, processes, and technologies consistent with the national information security program. Monitor compliance with judiciary technology policies and security standards. Complete the annual Judiciary IT Scorecard self-assessment. Develop and maintain security documentation including policies, procedures, guidelines, and checklists. Participate in the acquisition process following supply chain risk management practices and ensure procurements address security requirements. Prepare budget justifications for security initiatives and special management reports as needed. Coordinate IT disaster recovery and continuity planning, including maintaining recovery procedures, ensuring backup security, and supporting periodic testing.

- **Risk Assessment and Vulnerability Management:** Conduct security risk and vulnerability assessments of planned and installed information systems to identify weaknesses, risks, and protection requirements. Perform technical research to identify potential vulnerabilities and threats in existing and proposed technologies. Communicate findings and recommend mitigation strategies. Coordinate with the Circuit Executive's Office on risk management matters and contribute to the court's risk management framework. Participate in regular IT security and risk management meetings**.**

- **Project Coordination:** Plan and execute IT security projects, developing project plans, timelines, and resource requirements. Coordinate security-related aspects of broader ITO projects, ensuring security requirements are integrated throughout the project lifecycle. Provide regular project status updates and escalate issues through appropriate channels. Ensure project documentation and outcomes are communicated to stakeholders.

- **Technical Security Services:** Provide technical advisory services to securely design, implement, and maintain information technology systems, applications, cloud services, and network infrastructure. Ensure confidentiality, integrity, and availability of systems, applications, networks, and data across the system development lifecycle. Integrate security into system development by educating stakeholders and creating supporting methodologies and templates. Oversee implementation of security controls and generation of security documentation for system authorization.

- **Training and Awareness:** Conduct annual security awareness training for court staff. Provide security briefings, updates, and resources. Promote awareness and adoption of IT security best practices. Advise management on security needs, objectives, and vulnerabilities.

- **General Responsibilities:** Communicate and respond to judges, chambers staff, and management requests regarding court operations. Answer IT security questions for judges and staff, and the public. 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. Demonstrate sound ethics and good judgment at all times. Display a careful and deliberate approach in handling confidential information in a variety of contexts.

Required Qualifications

Education

At a minimum, candidates must possess a bachelor’s degree from an accredited college or university in computer science, information technology, cybersecurity, or similar field of study.

Specialized Experience

- **CL 26 ($62,212 – $101,109)**: Entry-level position. Candidates must possess at least one year of specialized experience in IT security. Experience must demonstrate knowledge of security principles, risk assessment, and vulnerability management, and ability to communicate technical information to varied audiences and work collaboratively within a team environment. Alternatively, candidates may qualify by completing a bachelor's degree with a major in cybersecurity, information assurance, or closely related field from an accredited college or university **and** superior academic achievement as listed below.
- **CL 27 ($68,346 – $111,099)**: At a minimum, candidates must possess at least two years of specialized experience in IT security. Experience must demonstrate knowledge of security principles, risk assessment, and vulnerability management, and ability to communicate technical information to varied audiences and work collaboratively within a team environment.
- **CL 28 ($81,906 - $133,178)**: Candidates must possess at least three years of specialized experience in IT security. Experience must demonstrate knowledge of security principles, risk assessment, and vulnerability management, and ability to communicate technical information to varied audiences and work collaboratively within a team environment. Specialized experience may be substituted by a master's degree from an accredited college or university in cybersecurity, information assurance, or closely related field.

Superior Academic Achievement

- An overall "B" grade point average equaling 2.90 or better of a possible 4.0; AND/OR
- Standing in the upper third of the class; AND/OR
- "3.5" average or better in the major field of study, such as Human Resources or a related field that would prepare a candidate well to perform in this position; AND/OR
- Election to membership in Phi Beta Kappa, Sigma XI, or one of the National Honorary Scholastic Societies meeting the minimum requirements of the Association of College Honor Societies, other than Freshman Honor Societies.
- Completion of one academic year (18 semester or 27 quarter hours) of graduate study at an accredited college or university. A degree program in cybersecurity, information assurance, or closely related field is preferred.

Preferred Qualifications

- Professional certifications: CISSP, CISM, CISA, Security+, or GIAC certifications
- Federal government or federal judiciary IT security experience
- Experience with NIST Cybersecurity Framework or similar security frameworks
- Experience conducting security assessments and supporting audit activities
- Project management experience or PMP certification
- Experience working within a management team structure and coordinating across functional areas

Application Process and Information

To be considered, application packages must be complete and submitted using the provided online application system which is accessible by following the link below. Complete packages must include:

1. Cover letter of no more than two pages, wherein the applicant describes the knowledge, skills, abilities, and/or experience that would make them well qualified to fill this position
2. Résumé outlining educational background, employment history, and other relevant information.
3. Academic transcripts.

4. Completion of the online AO-78, Federal Judicial Branch Application for Employment.
5. Completion of the online testing modules.

Once you have the cover letter, résumé, and academic transcripts (items 1, 2, and 3 above) readily accessible in PDF format, follow the link below to submit your files and complete the online AO-78 and online tests (items 4 and 5 above): https://www.ondemandassessment.com/o/JB-4REAC9LD4/landing

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. Applications submitted to this email address will not be reviewed.

Benefits Information

The candidate selected for this position will be eligible for a generous federal employee benefits package which includes:

- 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.
- 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. For in-person interviews, candidates must travel at their own expense. 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.

The position will report to downtown Washington, DC; however, limited telework may be available on an ad hoc basis and/or according to agency policy. Employees of the United States Court of Appeals for the Federal Circuit are excepted service, at-will appointments. Federal government civil service classifications or regulations do not apply. All offers of employment are provisional pending successful completion of a background check or investigation and a favorable employment suitability determination. Initial and continued appointment in this position is conditioned on a favorable moderate risk, five-year background investigation (renewed every five years). An unfavorable investigation at any point during employment may lead to removal. This position is subject to Electronic Funds Transfer (EFT) for payroll deposit.

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.