

OFFICE OF THE CIRCUIT EXECUTIVE
UNITED STATES COURTS OF THE
DISTRICT OF COLUMBIA CIRCUIT

Circuit IT Security Officer
Job Announcement Number USCA 25-07

Position Description - The Office of the Circuit Executive for the D.C. Circuit is accepting applications for the position of Circuit IT Security Officer (CISO). The CISO is in charge of IT security matters for the D.C. Circuit, which comprises the D.C. District Court, D.C. Court of Appeals, U.S. Probation Office, and various departments in the Circuit Executive office. The CISO provides advice to judges, senior court executives, and court employees on a wide range of IT security matters and is responsible for the management and implementation of IT security strategy, policies, protocols, procedures, systems, and training. The CISO serves as a strategic partner with executive management to assess organizational needs and build a culture that supports IT security best practices. The CISO collaborates with the Administrative Office of the United States Courts to assist with the implementation and creation of national security policies and the promotion of the Judiciary Information Technology Security Program. The CISO also works with other CISOs to collectively improve Judiciary security. This position reports directly to the Assistant Circuit Executive for IT. The position is full time and is located in Washington, D.C. Position is eligible for a hybrid work environment at the discretion of the Assistant Circuit Executive.

Duties and Responsibilities:

- Serve as an IT security expert supporting and assisting the D.C. Circuit's IT committee, judges, court unit executives, and IT staff on matters regarding IT security procedures and safeguards.
- Provide direct support and assistance to all court units within the D.C. Circuit on IT security related matters, including providing technical guidance and coordinating/conducting IT security assessments and training.
- Analyze and evaluate new and innovative information technology concepts, approaches, methodologies, techniques, services, guidance, training, and policies to enhance the information security posture of all departments within the D.C. 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.
- Establish mechanisms to promote awareness and adoption of security best practices. Conduct annual security awareness training for all Court of Appeals staff and provide frequent IT security briefings, updates, and other resources to all court units across the Circuit. Responsible for completion of the annual Judiciary IT Scorecard self-assessment and ensuring the Circuit is constantly enhancing its IT security posture.
- Serve with the ACE for IT as the liaison to the Administrative Office of the United States Courts on matters regarding IT security.
- Perform other functions as assigned.

Required Qualifications: The ideal applicant is a highly motivated professional who has an advanced understanding of computer hardware, software, and networks, as well as the theories, principles, practices, and techniques of data communications and network management, traffic, and security. The applicant should be exceptionally well-organized and innovative and possess outstanding written and oral communication skills, including the ability to communicate effectively with both technical and nontechnical persons. The applicant should have a bachelor's degree and at least four years of information technology security experience. Occasional travel is required.

Preferred Qualifications and Skills: The following knowledge, skills, and qualifications are highly desired:

- Bachelor's degree in computer science or business discipline.
- CISSP, CISM, CISA, or equivalent certification.
- Experience configuring, maintaining, and using Palo Alto Firewalls, SolarWinds, Nessus, Splunk, CyberArk, KACE, Qualsys, Forcepoint, Forescout, and other security tools.

Salary - CL 30 (\$113,975 to \$185,258) depending on qualifications.

Conditions of Employment - Applicants must be a United States citizen or eligible to work in the United States. Employees of the federal courts are excepted service appointments. Excepted service appointments are "at will" and may be terminated with or without good cause by the Court. The candidate selected for the position will be hired provisionally pending the results of a background investigation. Direct deposit of pay is required. Information about benefits is available at www.uscourts.gov/careers/benefits.

Application Process - Submit by email a cover letter and detailed resume. Email a single PDF attachment to VacancyCISO@cadc.uscourts.gov with the job announcement number in the subject line of the email. Because of the large volume of applications, only those candidates who will be interviewed will be contacted. Position is open until filled. The first cut-off date for review of applications is April 7, 2025.

<p>The Circuit Executive's Office is an Equal Opportunity Employer.</p>
--