



UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

IT SECURITY SPECIALIST

ANNOUNCEMENT NUMBER 24-WAW-24

ANNOUNCEMENT DATE May 15, 2024 / Open until filled; preference given to resumes received by June 7, 2024.

The United States District Court for the Western District of Washington is seeking a highly qualified IT Security Specialist. This position is part of a consolidated IT Department and reports to the IT Director. The incumbent performs work related to the implementation and administration of information technology security policies and practices in the U.S. District Court, including judicial chambers, Clerk's Office, U.S. Probation and Pretrial Services.

The IT Security Specialist performs professional work related to the management of information technology security policy, planning, development, implementation, training and support, and provides actionable advice to improve IT security and serves as a team lead to fulfill security objectives within the Court. The incumbent is responsible for developing and implementing local IT security policies, processes, and technologies that are consistent with the Federal Judiciary National Information Security program as well as for collaborating with other Judiciary stakeholders, such as the Administrative Office of the Courts (AO), Ninth Circuit, other Courts' IT personnel, and commercial IT resource providers.

This position is located at the federal courthouse in Seattle, Washington, with regular travel required to divisional offices, driver's license required. Part time telework may be considered depending on qualifications and experience.

REPRESENTATIVE DUTIES

- Collaborate and work with the IT Director and other IT team members to complete the annual judiciary IT security self-assessment program (Scorecard).
- Collaborate and work with the IT Director and the other IT team members to progress in closing the gaps in the CUSA (Court-Unit [IT] Security Assessment) findings. This includes monthly updates of the Plan Of Action & Milestones (POA&M).
- Lead, develop and work to initiate and track the annual IT Security Training for all units supported (KnowBe4). This includes ensuring users have completed the training within required deadlines. Track and provide guidance on the required bi-annual training for IT Staff, HR and other specialized personnel by the AO.
- Provide advice on matters of IT security, including security strategy and implementation, to judges, court unit executives, other senior court staff, and Systems Technology Division management. This includes leading and maintaining the judiciary security PII (Personally Identifiable Information) reduction and redaction program (DeleteMe).
- Lead and maintain the management and implementation of secured cloud storage services (Box.com).
- Lead and maintain the inventory disposal process, take the role of the disposal officer.
- Create and employ methodologies, templates, guidelines, checklists, procedures, and other documents in support of the court's IT security framework. Lead and facilitate the

review, update, and the approval process for security documents.

- Develop and administer local court security policies and guidance and assist with the remediation of identified risks and the implementation of security measures.
- Perform research to identify potential vulnerabilities in, and threats to, existing and proposed technologies, develop and implement effective mechanisms and procedures for mitigating risks and threats. This includes collaborate and work with the other team members in ushering patching priorities. This means scheduling monthly meetings and preparing reports of systems and vulnerabilities that need immediate attention or need priorities within 30-60 days or zero day.
- Attend the ISO (Information Security Office) meetings and other security related AO meetings and provide updates to the team either via email or during routine meetings with groups or individuals.
- Maintain and manage systems related to IT security within the court such as the Forcepoint server, vulnerability scanner servers, etc.
- May act as team lead or help the team lead in the administration of IT security-related automated tools including but not limited to antivirus products, operating system/software patch management mechanisms, web security/filtering platforms, system logging facilities, and locally installed firewall appliances.
- 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.
- Recommend and implement changes to ensure the reliability of information systems and to prevent and defend against unauthorized access to systems, networks, and data.
- Communicate and collaborate with other judiciary stakeholders including the Administrative Office, the Ninth Circuit IT Security Officer, other court IT personnel, and commercial IT resource providers regarding IT security guidelines, procedures, practices, administration, and incident response.
- Work with IT Management to complete the IT portion of the court's internal controls documentation, international travel policy and Continuity of Operations documentation.
- Work with the CST team and Lead Training Specialist to educate judges about IT security best practices when traveling.
- Other duties as assigned.

QUALIFICATIONS

- Possess technical knowledge and at least 3 years of work experience in network management and security, network traffic analysis, computer hardware and software, and data communications.
- Ability to identify and analyze security risks and implement resolutions.
- Ability to detect, identify, and analyze IT security problems and assess the implications of alternative solutions.
- Knowledge and experience of anti-malware and endpoint security controls.
- Knowledge of IPSec and the ability to use it to protect data, voice, and video traffic.
- Skill in designing security architecture roadmaps and documenting architecture decisions.
- Strong technical writing skills.
- Ability to write, analyze, design and implement security policies and procedures.

<p>PREFERRED QUALIFICATIONS</p>	<ul style="list-style-type: none"> • Knowledge and at least 3 years of professional experience in the installation, configuration, and support of Windows Server operating systems, Microsoft Active Directory, and Windows 10/11 desktop operating systems for enterprise of at least 100 users; Working experience of enterprise IT asset management and patch deployment utilities such as Microsoft System Center Configuration Manager, Websense/Forcepoint Triton web security platform, Enterprise log management/analysis platforms including Splunk and Nessus, and Network monitoring solutions such as SolarWinds. • Strong customer service skills; the ability to work cooperatively with clients, team members, and managers; • The ability to move projects forward and track multiple priorities in a fast-paced environment; and the ability to follow an assigned project through to completion. • Experience in a federal court environment and/or experience with specialized applications designed for the federal courts. • A bachelor’s degree from an accredited college or university • CISSP Certified or Security+ Certified or Network+ Certified
<p>SALARY RANGE</p> <p>INFORMATION FOR APPLICANTS</p> <p>BENEFITS</p>	<p>Court Personnel System Classification Level: CL27, Step 1 – 61, \$64,980 - \$105,636 annually CL28, Step 1 – 61, \$77,880- \$126,620 annually CL29, Step 1 – 61, \$92,624 - \$150,547 annually</p> <p>Qualified applicants should submit the following:</p> <ul style="list-style-type: none"> • Cover letter • Resume • AO78 Form (Application for Employment) - <i>For this vacancy announcement (24-WAW-24), you do not need to complete the optional background information – questions 18, 19, and 20.</i> <p>All documents listed above must be submitted for the applications to be considered complete. Incomplete applications will not be considered for the next steps in the recruitment process. Please submit completed application packets as a single Word or Acrobat .pdf document via e-mail to: seattle_personnel@wawd.uscourts.gov</p> <p>Or to: Human Resources (#24-WAW-24) U. S. District Court 700 Stewart Street, Suite 2218 Seattle, WA 98101</p> <p>The District Court offers a generous benefit package, competitive salary, and a dedication to work/life balance including flexible schedules, ORCA transit passes, and telework opportunities. Judiciary employees participate in the Federal Employees Retirement System, Thrift Savings Plan (similar to a 401K), health and life insurance benefits, long term care options, annual sick leave accrual, and eleven paid holidays per year. Judiciary employees are eligible for student loan forgiveness for qualifying Federal student loans. Judiciary employees are <u>not</u> covered by the Office of Personnel Management’s civil service classification system or regulations. For additional information on employment with the federal courts, please visit www.uscourts.gov.</p>

**INFORMATION FOR
APPLICANTS**

Only qualified applicants will be considered for this position. Applicants must be United States citizens or eligible to work in the United States. Employees of the United States District Court are considered “at will” employees. Applicants selected for interviews must travel (for in-person interviews) or connect via Zoom (for remote interviews) at their own expense.

The United States District Court requires employees to follow the [Code of Conduct for Judicial Employees](#). Reference checks with current and former employers will be conducted on top candidates. A background investigation with law enforcement agencies, including fingerprint and criminal record checks, will be conducted as a condition of employment. Any applicant selected for a position will be hired provisionally pending successful completion of the investigation. Unsatisfactory results may result in termination of employment.

The Federal Financial Management Reform Act requires direct deposit of federal wages.

The United States District Court for the Western District of Washington is an Equal Opportunity Employer. We encourage applications from all qualified individuals and seek a diverse pool of applicants in terms of race, ethnicity, national origin, sex, gender identity and expression, sexual orientation, age, languages spoken, veteran’s status, disability, religion, and socio-economic circumstance.

The Court provides reasonable accommodations to applicants with disabilities. If you need a reasonable accommodation, please notify Human Resources. The decision on granting reasonable accommodations will be made on a case-by-case basis.

The Court reserves the right to modify the conditions of this job announcement, to withdraw the announcement, or to fill the position sooner than the closing date, any of which may occur without prior written or other notice. If a position becomes vacant in a similar classification, within a reasonable time from the original announcement, the Clerk’s Office may select a candidate from the applicants who responded to the original announcement without posting the job announcement again.

The United States District Court is an equal opportunity employer and values diversity in the work place.