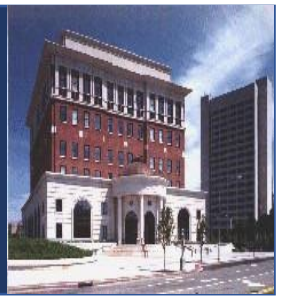
UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF
NEW YORK



Position: IT Security Officer (Shared Services)

Vacancy No. 26-30

Location: 500 Pearl Street, New York, NY

Term: Permanent

Class Level: CL - 29

Salary Range: $100,335- $163,075 per annual

(Starting salary for non-Federal employees: $100,335–$125,431 depending on work experience and qualifications)

Opening Date: 08/13/2026

Closing Date: Open until filled (with preference set for 09/10/2026)

BENEFITS:

- Paid Annual & Sick Leave
- 11 Paid Holidays
- Employer subsidized Health Insurance
- Group Life Insurance
- Supplemental Vision/Dental Insurance
- Retirement Benefits Plan (FERS)
- Thrift Savings Plan (TSP)
- Flexible Spending Accounts
- Transit Subsidy Program (pursuant to eligibility requirements)
- Onsite fitness center
- Pre-tax benefit programs
- Employee assistance program (EAP)
- Mandatory enrollment in electronic funds transfer (EFT) for net pay

CONDITIONS OF EMPLOYMENT:

Applicants must be U.S. citizens or lawful permanent residents seeking U.S. citizenship.

POSITION OVERVIEW: The United States District Court for the Southern District of New York is accepting applications for a Shared Services IT Security Officer to serve multiple Court units, specifically, the Clerk's Office and Probation Office. We seek a seasoned professional who will pro-actively advance security priorities and engage customers in security awareness, training, and best practices. The selected candidate will be a self-starter who will improve the district's security posture. As part of several information technology teams, the incumbent will work in a professional work environment to deliver impactful security initiatives for the district. Secondary responsibilities include assisting the network administrators in the administration of the judiciary's information technology network by developing standards, recommending network infrastructure change, and participating in the high-level and long-term design and analysis of the courts' network and data systems from a security perspective. Work hours are 8:30a.m. – 5:00p.m. with some flexibility and may require some after hours and weekend availability. This position may be eligible for occasional telework, in accordance with the Court's telework policy. A mobile phone will be provided.

DUTIES AND RESPONSIBILITIES: The IT Security Officer performs professional work related to the management of information technology security policy, planning, development, implementation, training, and support for the Clerk's Office and Probation Office. The incumbent provides actionable advice to improve IT security and serves as a team lead to fulfill security objectives within the court. The incumbent ensures the confidentiality, integrity, and availability of systems, networks, and data across the system development life cycle, and creates, promotes, and adheres to standardized, repeatable processes for the delivery of security services. The IT Security Officer pro-actively engages all users in security awareness and training activities to promote the appropriate use of best security practices within the court. The incumbent is responsible for implementing local security policies, processes, and technologies that are consistent with the national Information Security program as well as for collaborating with other judiciary stake holders, such as the Administrative Office and other court IT personnel, to identify and collectively advance security initiatives both within and beyond court unit boundaries.

CONDITIONS OF EMPLOYMENT (continued):

In order to be compensated with appropriated funds for a position within the continental United States, applicants must be:

(1) U.S. citizen,

(2) Lawful permanent resident (i.e., green card holder) who is seeking citizenship as outlined in 8 U.S.C. §1324b(a)(3)(B).

Note: Some noncitizen applicants who are permanent residents may not yet be eligible to apply for citizenship at the time they begin. Such individuals may still lawfully be employed if they provide an affidavit indicating that they intend to apply for citizenship when they become eligible to do so.

Employees of the United States District Court are not included in the government's Civil Service classification and are at-will employees.

All employees, interns and volunteers are required to adhere to the Code of Conduct for Judicial Employees available for public review on the **USCourts.gov website**.

The successful candidate for this position is subject to a Background check investigation for high-sensitive clearance. This position is subject to mandatory electronic funds transfer for payment of net pay.

*All internal applicants will receive an email confirming receipt of their application. If confirmation is not received within two days after the vacancy closes, please contact Human Resources.

REPRESENTATIVE DUTIES:

- Review, evaluate, and make recommendations on courts' technology security programs.
- Create and employ procedures, templates, guidelines, and other documents to establish repeatable processes across the district's information technology security services.
- Serve as the primary implementer of all security initiatives and provide direct hands-on effort when implementing security programs, projects and solutions.
- Proactively track, triage, and remediate identified security risks and implement security measures. Coordinate the remediation of larger security risks with other IT team members and advise management when additional resources are needed.
- Perform research to identify potential vulnerabilities in, and threats to, existing and proposed technologies, and notify the appropriate managers/personnel of the risk potential. Conduct security risk and vulnerability assessments. Perform routine scans and remediations to system vulnerabilities and monitor for outdated applications and security-related matters.
- Communicate and provide advice on matters of IT security, including security strategy and implementation to judges, court unit executives, and other court staff managers.
- Assist in the development and maintenance of local court unit security policies and guidance. Serve as a resource to all court units within the district regarding federal and judiciary security regulations and procedures.
- Manage information security projects (or security-related aspects of other IT projects) to ensure milestones are completed in the appropriate order, promptly, and according to schedule. Facilitate project meetings. Prepare justifications for budget requests. Prepare special management reports as needed.
- Establish mechanisms to promote security. Train court staff on security awareness and adoption of security best practices using available tools and resources.
- Serve as a 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.
- Assist with special projects as directed by management and perform other IT support duties as assigned.
- Act as the primary contact for internal/external security assessments and audits and, address relevant issues found.
- Perform analysis, remediation, forensics, and any other activities need concerning any IT security incidents.
- Coordinate with local IT staff and the judiciary Security Operations Center to resolve issues and take any required action, immediate or otherwise.

The Southern District of New York values diversity and is committed to inclusion in the workplace. We encourage applications from all qualified individuals and seek a diverse pool of applicants.

Visit our website:

REQUIRED QUALIFICATIONS: To be considered for this position you must be a high school graduate, or equivalent. To qualify for the CL-29 level, you must have two years of specialized experience.

SPECIALIZED EXPERIENCE: Progressively responsible experience that is in, or closely related to, the work of the position that has provided the knowledge, skills, and abilities to successfully perform the duties of the position. to successfully perform the duties of the position. Incumbent must have specialized experience to include the following:

- Experience with IT security tools and the ability to learn new tools and methods.
- System administration experience.
- Ability to perform independent research and identify training needs.
- Ability to collaborate with individuals, teams of any size, and organizations of any size.
- The ability to work with other local and remote technical staff to identify, prioritize, and resolve security issues - especially those identified in security scans.
- Good judgment, be dependable, be a proactive self-starter, and demonstrate initiative in problem-solving.
- Exceptional ability to effectively communicate, articulate, and relate to coworkers and others with professionalism and integrity.

*Specialized work experience attained outside the Federal Judiciary may be creditable, but that experience must be documented on Form AO78 to be evaluated.

PREFERRED QUALIFICATIONS:

- A degree from an accredited university in a field related to the discipline is preferred.
- Experience with IT security tools used by the US Courts (Splunk, Trend Micro, Forcepoint Nessus, KACE, VMware VRa8 and CIS Critical Security Controls v8).
- Experience in, or with, the US Courts, government or large organizations.
- Ability to create and maintain policies, end-user documentation, and instructions.
- Ability to perform internal IT security assessments and self-audits, and monitor policy adherence, understanding of CIS Critical Security Controls v8 (Center of Internet Security).
- Knowledge of data backup systems (Backup Exec, Veeam, VM snapshots).
- Security-related certifications (e.g., CISSP, Security+, CISM) are highly valued.

PREFERRED KNOWLEDGE, SKILLS AND ABILITIES:

COURT OPERATIONS: Knowledge of or the ability to learn court operations, functions, and organizational structure.

INFORMATION TECHNOLOGY, SECURITY AND AUTOMATION: Knowledge and expertise in the theories, principles, practices and techniques of network management and security, IT networks, network traffic, computer hardware and software, and data communications. Knowledge of applicable programming languages, such as Visual Basic, Java, PHP, and SQL. Ability to analyze IT security problems and assess the practical implications of alternative solutions. Ability to identify and analyze security risks and to implement resolutions. Knowledge of anti-malware and endpoint security controls.

EQUAL OPPORTUNITY EMPLOYER

The U.S. Federal Courts are committed to equal employment opportunity without regard to race, color, religion, national origin, sex, age, disability, or any other protected characteristic.

PREFERRED KNOWLEDGE, SKILLS AND ABILITIES (continued):

Knowledge of IPSec and the ability to use it to protect data, voice, and video traffic. Ability to work with other court divisions within the circuit in order to collaborate on best practices. Skill in designing security architecture roadmaps and documenting architecture decisions. Thorough understanding of IT policies and procedures.

PROJECT MANAGEMENT: Ability to assist in leading and providing hands on support for security projects, including organization knowledge, analysis, documentation, reporting, recommending, and strategic thinking. Skill in resolving technical, administrative, and operational problems, providing recommendations to users, service providers, and senior management. Will be involved in directly implementing solutions on systems and processes. Demonstrated ability to effectively analyze and synthesize diverse input, establish priorities, and complete multiple projects. Knowledge and understanding of the steps required in developing secure IT systems and making modifications to ensure that appropriate security measures are in place and are enforced.

JUDGMENT AND ETHICS: Ability to consistently demonstrate sound ethics and judgment, maintain court confidentiality and security requirements, and comply with the Code of Conduct for Judicial Employees.

WRITTEN AND ORAL COMMUNICATION: Must have excellent interpersonal skills and be able to effectively communicate (orally and in writing) to individuals and groups to provide information and reports in understandable format. Ability to interact professionally with a wide variety of stakeholders, providing exceptional customer service and resolving difficulties while complying with regulations, rules, and procedures. Ability to provide and exchange accurate and timely information with individuals within and outside the court.

APPLICATION PROCEDURE:

To be considered for this position, please submit your:

1. Resume detailing your education and work experience.
2. A cover letter. The cover letter must indicate the position for which you are applying, including the vacancy number, and identify how your education and/or experience relate to the duties and responsibilities of the position.
3. AO78 Application for Federal Employment. The Application for Federal Employment (AO78) can be downloaded from: www.uscourts.gov/forms-rules/forms/application-judicial-branch-federal-employment.

Only applications submitted via email will be accepted. It is preferred for the applications to be submitted in a single PDF document, and for candidates to include the vacancy number and position title in the subject field of the email containing the application. Applications submitted as zip files, cloud files and/or links will not be accepted. Applications that do not conform to the above procedures will not be considered. Only candidates selected for the interview process will be contacted. Please submit your application to:

Careers@nysd.uscourts.gov