UNITED STATES DISTRICT COURT DISTRICT OF CONNECTICUT
VACANCY ANNOUNCEMENT - USDC-CT 17-16

POSITION: IT Security Officer
SALARY RANGE: CL 29 ($78,281 - $127,252)
DUTY STATION: New Haven, CT

OPENING DATE: November 3, 2017
CLOSING DATE: November 24, 2017

The United States District Court for the District of Connecticut is seeking a full-time Information Technology (IT) Security Officer. The IT Security Officer performs professional work related to the management of IT security policy, planning, development, implementation, training, and shared services support for all court units within the District of Connecticut. The incumbent provides actionable advice to improve IT security and serves as a team lead to fulfill security objectives. The incumbent also ensures the confidentiality, integrity, and availability of systems, networks, and data across the system development life cycle (SDLC), and creates, promotes, and adheres to standardized, repeatable processes for the delivery of security services. The IT Security Officer also collaborates with the Administrative Office (AO), while working with local court units, to collectively establish and raise the security baseline of the Judiciary.

Representative Duties:

- Review, evaluate, recommend, and enact change on the district's technology security programs. Promote and provide support of existing information security services.
- Provide technical advisory and remediation services to securely design, implement, maintain, or modify IT systems and networks. Perform research to identify potential vulnerabilities in, and threats to, existing and proposed technologies, and notify the appropriate personnel of the risk potential.
- Provide advice on matters of IT security, including security strategy and implementation, to judges, court unit executives, and other senior staff. Serve as an information security resource regarding federal and judiciary security regulations and procedures.
- Assist in the development and maintenance of local court unit security policies and guidance, the remediation of identified risks, and the implementation of security measures.
- Develop, analyze, and evaluate new and innovative information technology concepts, approaches, methodologies, technologies, techniques, services, guidance, and policies that will constructively transform the district's information security posture. 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 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.

- Oversee and enact the implementation of security measures on information systems and generate security documentation for system authorization and operation.
- Manage information security projects (or security-related aspects of other IT projects) to ensure milestones are completed in the appropriate order, in a timely manner, and according to schedule. Serve as a liaison with stakeholders to integrate security into the system development lifecycle. Facilitate project meetings, educate project stakeholders about security concepts, and create supporting methodologies and templates to meet security requirements and controls.
- Assist in developing policies and procedures to ensure information systems reliability and prevent and defend against unauthorized access to systems, networks, and data.
- Create and employ methodologies, templates, guidelines, checklists, procedures, and other documents to establish repeatable processes across the district's IT security services.
- Establish mechanisms to promote awareness and adoption of security best practices.
- Oversee and execute internal assessment framework tasks, including: log management review, physical security monitoring/auditing, patch management, etc.
- Prepare justifications for budget requests.
- Prepare special management reports as needed.
- Other duties as assigned.

Education/Experience:

High School diploma required, Bachelor's degree or higher from an accredited institution preferred. Additionally, Certified Information Systems Security Professional (CISSP), Certified Information Security Management (CISM), Certified Information Systems Auditor (CISA), CompTIA Security+, or similar certification(s) is desired.

Incumbent must have at least five years of professional IT security experience. Such experience may include:

- Thorough knowledge of IT systems and network security, network traffic analysis, computer hardware and software, and data communications.
- Designing IT security awareness training programs for users and IT staff with application of industry standards.
- Ability to identify and analyze security risks and to implement resolutions.
- Knowledge of anti-virus, anti-malware, application control, web threat protection and endpoint security controls. Knowledge of and experience with enterprise-level firewalls (Cisco ASA / Palo Alto). Understanding of incident response processes, including the ability to implement plans and procedures.
- Knowledge of and experience with the following software platforms:
    - Log Management (Splunk);
    - IDS/IPS (Snort);
    - Patch Management (Dell KACE/WSUS); and
    - Vulnerability Scanning (Nessus).
- Skill in interpersonal communications, including the ability to use tact and

diplomacy in dealing effectively with all levels of management, staff, and judicial officers.
- Skill in project management, organizing information, managing time and multiple work assignments effectively, including prioritizing and meeting tight deadlines.
- Understanding of applicable programming languages, such as Python, Java, PHP, and SQL, with experience in providing risk assessment and risk mitigation strategies.

How to Apply:

Submit resume, with cover letter detailing why you believe your qualifications match the requirements of this position. Please submit a completed application for judicial branch employment, Form AO 78A (available at http://www.uscourts.gov/forms/AO078.pdf) **by email only**, to:
Human Resources Department @ Email: **HR_department@ctd.uscourts.gov**

Submit a written narrative discussing, in your opinion, two of the largest challenges organizations face regarding IT security and what can be done to address them. Discuss the primary reason(s) organizations have not addressed vulnerabilities and what approach can be taken to help correct that. Additionally, review the principle areas identified below and choose two areas which you feel are most important in the role of IT security. Submit an additional statement addressing your skill, experience, and abilities in the two areas you selected.

- System/Software Inventory and Data Identification
- Policy Creation and Enforcement
- Privileged Account Access Management
- Password Security Management
- Web-based Threat Protection
- Patch Management
- Security Training (Executive and Line Staff)
- Physical Security
- Anti-virus / Anti-Malware Protection
- Enterprise Log Management
- Network Perimeter Protection
- Data Resiliency

Conditions of Employment:

- Applicants must be U.S. citizens or eligible to work in the United States***.***

- Successful candidate is subject to a full fingerprint and background records check. Any applicant selected for a position will be hired provisionally pending successful completion of the background investigation.

- Mandatory electronic direct deposit of salary payment.

- Employees are required to adhere to the Code of Conduct for Judicial Employees [available to applicants to view at the court website: www.ctd.uscourts.gov].

- Employees of the U.S. District Court are EXCEPTED SERVICE APPOINTMENTS. Excepted service appointments are “at will” and can be terminated with or without cause by the court.

- All applications will be reviewed to identify the best qualified candidates. Due to the volume of applications received, the Court will only communicate with those individuals invited for an interview. Applicants selected for interviews must travel at their own expense. The Court may close this announcement at any time. The Court reserves the right to modify the conditions of

this position announcement or to withdraw the announcement, which may occur without prior written notice.

The United States District Court is an Equal Opportunity Employer.