UNITED STATES DISTRICT COURT - EASTERN DISTRICT OF VIRGINIA

www.vaed.uscourts.gov

JOB OPPORTUNITY NUMBER: FY 19-004

POSITION: IT Security Officer

LOCATION: Norfolk Division

Opening Date: November 8, 2018

Closing Date: Open until filled. Applications received by November 30th will receive first consideration.

CLASSIFICATION LEVEL/STARTING SALARY: CL 28-CL 29 ($58,700 - $113,459)
Actual starting salary dependent upon qualifications.

POSITION OVERVIEW

The United States District Court for the Eastern District of Virginia 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 the United States District Court and Probation Office. 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. **Some travel required.**

DUTIES AND RESPONSIBILITIES

- 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.
- Assist the network team
- Prepare special management reports as needed.
- Other duties as assigned.

QUALIFICATIONS
- Minimum of five years of professional IT experience including at least one year equivalent to work at CL 27.
- Thorough knowledge of IT systems and network security, network traffic analysis, computer hardware and software, and data communications.
- Knowledge of anti-virus, anti-malware, application control, web threat protection and endpoint security controls. Knowledge of and experience with enterprise-level firewalls. Understanding of incident response processes, including the ability to implement plans and procedures.
- 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.
- Thorough understanding of IT security theories and best practices, as well as an ability to assist with analysis, design, and implementation of security policies and procedures.
- Knowledge of and experience with the following software platforms:
    - Log Management;
    - IDS/IPS;
    - Patch Management; and
    - Vulnerability Scanning.
- Excellent written and oral communication, presentation, and organizational skills.
- The ability to use tact and diplomacy in dealing effectively with all levels of Court personnel.
- The ability to work independently and in a team environment.
- Skill in project management, organizing information, managing time and multiple work assignments effectively, including prioritizing and meeting tight deadlines.
- Understanding of applicable programming languages and SQL.
- Ability to lift up to 40lbs.

EDUCATION
High school graduation or equivalent required. College degree preferred.

Certified Information Systems Security Professional (CISSP), Certified Information Security Management (CISM), Certified Information Systems Auditor (CISA), CompTIA Security+, or similar certification(s) is desired.

Completion of a master's degree or two years of graduate study (27 semester or 54 quarter hours) in an accredited college or university in information technology, business or public administration, education, industrial relations, psychology, or other field closely related to the subject matter of the position may be substituted for two years of specialized experience.

BENEFITS
This position is covered by the Court Personnel System. A generous benefits package is available to full-time permanent employees that includes:

- A minimum of 10 paid holidays per year
- Paid annual leave in the amount of 13 days per year for the first three years, 20 days per year after three years, and 26 days per year after fifteen years
- Paid sick leave in the amount of 13 days per year
- Retirement benefits
- Optional participation in Thrift Savings Plan
- Optional participation in choice of Federal Employees' Health Benefits
- Optional participation in the choice of Supplemental Dental and Vision Insurance
- Optional participation in choice of Federal Employees' Group Life Insurance
- Optional participation in the Flexible Benefits Program
- Optional participation in the Commuter Benefit Program
- Optional participation in Long-Term Care Insurance
- Optional participation in private long-term disability plan
- Credit for prior government service

CONDITIONS OF EMPLOYMENT
Employees must be United States citizens or eligible to work in the United States.

Employees are required to adhere to the Code of Conduct for Judicial Employees, which is available to applicants to review upon request.

Employees of the United States District Court are **Excepted Service Appointments.** Excepted service appointments are at will and can be terminated with or without cause by the Court.

Employees will be hired provisionally pending the results of a background investigation.

Employees are required to use the Electronic Fund Transfer (EFT) for payroll deposit.

APPLICATION INFORMATION
Interested applicants must submit a cover letter, resume, a list of professional references, and the Application for Federal Employment which is located under "Related Links" on the Employment page of our website (Please use the Word version if using a Mac computer). **In addition,** applicants must submit narrative statement 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 may not be able to address vulnerabilities and what approach can be taken to help correct that.

To ensure consideration, application packages with all the required materials must be received by **November 30th, 2018.** Submit electronically to ITJOBS@vaed.uscourts.gov .

Only applicants selected for an interview will be notified. Remaining applicants will not receive notice.

The United States District Court is an Equal Opportunity Employer