

UNITED STATES DISTRICT COURT - EASTERN DISTRICT OF VIRGINIA

www.vaed.uscourts.gov



JOB OPPORTUNITY NUMBER: FY 17-014

POSITION: IT Security Specialist

LOCATION: Norfolk Division

Opening Date: September 13, 2017

Closing Date: Open until filled.

Applications received by October 6 will receive first consideration.

CLASSIFICATION LEVEL/STARTING SALARY: CL 26 (\$43,840 - \$71,247)

POSITION OVERVIEW

This position is located within the Eastern District of Virginia Consolidated Information Technology Department which serves judges, judicial staff, and the staffs of the Clerk's Office and the U.S. Probation Office. Manages and guides the maintenance of systems to protect data from unauthorized users. Monitor and report on network, systems, and desktop applications for security events. Evaluate security products to ensure compatibility with information security policies. Performs routine audits and vulnerability scans to ensure compliance with security policy. Participates in audits or reviews of desktop systems, operations methods, and risk assessments. Assists in the development of policy related to desktop security. **Some travel required.**

DUTIES AND RESPONSIBILITIES

- Assist in planning, coordinating, and implementing security measures to protect information and information processing assets.
- Works with Network Engineer on the design and implementation of network control mechanisms to control access to computer networks.
- Manages threats, vulnerabilities, and incidents impacting end user information resources through vulnerability assessments and other security tools and audits of the Incident Response Plan. Provides summaries of findings to IT management.
- Manages Courts endpoint security programs.
- Assure through policies the appropriate use of information resources. Perform audits throughout the year to validate policies.
- Manage and oversee the manual and automated log review, performing analysis and related control techniques to identify, assess, prioritize and communicate technical information security risks to IT management and staff for appropriate response.
- Participate in the installation and update of software and patches as well as maintenance of the Configuration Management Plan to ensure a consistent secure baseline image and adherence to the Courts Patch Management Plan.
- Responsible for implementation of the Courts security awareness training program. This includes developing and providing the annual security awareness program, documenting attendance, and providing additional security information ad hoc during the year.
- Responsible for recommending, documenting, and managing mobile device security, biometric access, and password management programs.
- Provide end user support for applications supported. Serve as liaison between IT management and end users.
- Monitor day-to-day operations of technology equipment and its systems. Serve as the technical expert in solving computer system problems.
- Backs up the other IT staff and performs other office automation, user support, and project duties for the consolidated IT department as necessary.

QUALIFICATIONS

- Minimum of two years of professional IT experience including at least one year equivalent to work at CL-25.
- In-depth knowledge of computer hardware, software, networks.
- Working knowledge of theories, principles, practices, and techniques of data communications and network management, traffic, and security.
- 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.
- Experience with deployment and management of anti-malware and endpoint security controls.
- Experience with IDS/IPS, Splunk and/or other tools used to monitor network or system activities for malicious activities or policy violations and produces reports to a management.
- 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.
- Ability to lift up to 40lbs.

EDUCATION

High school graduation or equivalent required. College degree preferred. Knowledge or certifications at the Security+ or CISSP level preferred.

Education may be substituted for one year of specialized experience as follows:

Completion of the requirements for a bachelor's degree from an accredited college or university **and** one of the following superior academic achievement requirements:

- An overall "B" grade point average equaling 2.90 or better of a possible 4.0;
- "3.5" average or better in the major field of study related to this position, such as information technology, business or public administration, education, industrial relations, or psychology; or
- Completion of one academic year (18 semester or 27 quarter hours) of graduate study in an accredited university in business or public administration, information technology, business or public administration, information technology, psychology, or other field closely related to the subject matter of the position.

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, the Application for Federal Employment (document can be found under “Related Links” on the Employment page of our website - please use the Word version if using a Mac computer), and a list of references. In addition, applicants must submit narrative statements that answer the following questions:

1. Cybersecurity relies on the concept of defense in depth to protect data and technology assets. If you had to choose one component or layer as the most important, which would you choose and why?
2. As the IT Security Specialist you will need to review many events in logs and endpoint security products. In your opinion, when does an event become an incident?

To ensure consideration, applications must be received by **October 6, 2017**. Submit electronically to: ITSS@vaed.uscourts.gov. Hard copies and faxed copies will not be accepted.

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

The United States District Court is an Equal Opportunity Employer