

CAREER OPPORTUNITY (Temporary to Permanent Possible)



Probation Office District of South Carolina

Vacancy #:	2020 - DSC - 01
Position:	IT Security Specialist
Location:	Columbia, South Carolina
Salary:	CL 28 (\$ 61,360 - 99,762) <i>based on qualifications</i>
Date Posted:	January 21, 2020
Closing Date:	Open until filled
	Preference given to applications received prior to February 11, 2020.

Position Summary

The District of South Carolina is seeking a talented IT Security Specialist to serve the Probation and Pretrial Services Offices. The successful applicant's office location will be in Columbia, SC. We are looking for an IT professional who can pro-actively advance security priorities, engage customers in security awareness, and can perform information security duties as a primary role. This position will report to the IT Manager. The Information Technology Team in the District of South Carolina supports a staff of approximately 140 in six (6) locations across the state. The district is looking for a self-starter who will improve the district's security posture and collaborate with other regional and national judiciary stakeholders. As part of the Information Technology Team, you will work in a professional work environment to deliver impactful security initiatives for the district which will also support national programs. The incumbent provides actionable advice to improve IT security and serves as a team member to fulfill security objectives.

Summary of Representative Duties and Responsibilities

- Review, evaluate, and make recommendations on technology security programs. Create and employ procedures, templates, guidelines, and other documents to establish repeatable processes across the district's information technology security services.
- Proactively monitor, scan, track, and remediate identified security risks and implement security measures. Coordinate the remediation of larger security risks with the IT team.
- 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 Perform routine scans and remediations of system vulnerabilities and monitor for outdated applications and security-related matters.
- Develop, analyze, and evaluate new and innovative achievable technology concepts, approaches, methodologies, technologies, techniques, services, and guidance that will constructively transform the district's information security posture.
- Communicate and provide advice on matters of IT security, including security strategy and implementation to managers, as appropriate

- Assist in the development and maintenance of local security policies and guidance, as requested. Serve as a resource within the district regarding 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.
- Prepare cost analysis and/or justifications for budget requests for information security related purchase requests.
- Establish mechanisms to promote security. Train court staff on security awareness and adoption of security preferred practices.
- Serve as a team member 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 a key contact for external security assessments and audits, and address relevant issues found. Ability to understand, define, and document risk acceptance matters.
- Perform analysis, remediation, and other activities concerning IT security incidents.

Required Qualifications

- To qualify at the CL-28, the applicant must have a bachelor's degree from an accredited college or university plus a minimum of two years of previous IT work experience inclusive of work related to Information Security.
- Individual must be able to lift and move equipment up to 40 pounds.
- Experience with various IT security tools and the ability to learn new tools and methods.
- Firewall work experience
- Scanning tools familiarity
- Networking infrastructure knowledge
- Basic competency in Microsoft Office Products
- Ability to perform independent research and identify training needs.
- Ability to collaborate with individuals and teams of varying sizes.
- The ability to work with other local and remote staff to identify, prioritize, and resolve security issues, especially those identified in security scans.
- Good judgment, dependable, a proactive self-starter, and demonstrate initiative in problem-solving.
- Exceptional ability to effectively communicate, articulate, and relate to co-workers and others with professionalism, tact, positive attitude, and integrity
- Travel and overnight stays, at times, may be required.

Desired Qualifications

- Experience with specific IT security tools such as Splunk, Nessus, KACE (or other Patch Management), and Forcepoint/WebSense
- Ability to create and maintain end-user documentation and instructions
- Ability to perform internal IT security assessments and self-audits
- U.S. Courts experience

Benefits

Federal benefits include paid vacation and sick leave, paid holidays, and retirement benefits. Optional benefits include health and life insurance, disability and long-term care insurance, dental and vision insurance, and a tax-deferred savings plan. This position is subject to mandatory electronic fund transfer (direct deposit) participation for payment of net pay.

Procedures for Applying

To be considered for this position, please visit our website at:

<https://www.scp.uscourts.gov/career-opportunities>

Submit via email (or postal mail) and attach:

1. Cover letter that describes your interest in pursuing this position and how your experience relates to the stated duties, responsibilities, skills, and abilities of this position.
2. Judicial Branch Federal Employment Application (AO78). The AO78 is located on our website.
3. Resume.
4. College transcripts.
5. Last 2 performance evaluations.
6. USPO Release form and Equifax Release form (located on our website).
7. A short (no more than one page) narrative describing your philosophy on security policy adherence, operational risk acceptance, and how you keep abreast of changes.

Incomplete application packets will not be considered.

E-mail application packets to: SCP_HR@scp.uscourts.gov or mail to:

Patti K. Rabon, Personnel Specialist
U.S. Probation Office
1835 Assembly Street, Room 611
Columbia, SC 29201

Please note:

The court is not authorized to reimburse candidates for travel in connection with an interview or to pay relocation expenses to the successful candidate.

As a condition of employment, the selected candidate must complete a background check investigation, including an FBI fingerprint check. All court employees are *at will*, and therefore the selected candidate may be removed from this position at any time if the selected candidate fails to perform at a satisfactory level. In addition, employees are required to adhere to the *Code of Conduct for Judicial Employees*.

The Court reserves the right to modify the conditions of this job announcement or to withdraw the job announcement, or to fill the position sooner than the closing date, any of which action may occur without any prior written notice. Only applicants who are interviewed in person will receive a written response regarding their application.

The United States District Court is an Equal Opportunity Employer