UNITED STATES BANKRUPTCY COURT
EASTERN DISTRICT OF CALIFORNIA

POSITION ANNOUNCEMENT #19-6

POSITION:	**IT Security Administrator**
LOCATION:	**Sacramento, CA**
SALARY RANGE:	**$64,777 – $125,202 (CL 28/29)** **Depending on Experience**
OPENING DATE:	**June 11, 2019**
CLOSING DATE:	**July 10, 2019**

Position Overview

The United States Bankruptcy Court is seeking an IT Security Administrator in Sacramento, CA. This position is part of an Information Technology team and will be shared with the U.S. Probation Office and the U.S. Pretrial Services Office. The IT Security Administrator performs professional work related to the management of information technology security policy, planning, development, implementation, training, and support, and provides actionable advice to IT security policies, processes, and technologies that are consistent with the federal judiciary national Information Security program. While this position is full-time, it is not a permanent position. The estimated longevity of the position is two to three years, subject to funding.

Representative Duties

- Review, evaluate, and make recommendations on the court's technology security program, including automation, telecommunications, and other technology utilized by the court. Promote and support security services available throughout the district.
- Provide technical advisory services to securely design, implement, maintain, or modify information technology systems and networks that are critical to the operation and success of the court units. Perform research to identify potential vulnerabilities in, and threats to, existing and proposed technologies, and develop and implement effective mechanisms and procedures for mitigating risks and threats. Notify the appropriate managers/personnel of IT asset security vulnerabilities.
- Provide advice on matters of IT security, including security strategy and implementation, to judges, court unit executives, and other senior court unit staff.
- Develop and administer local court security policies, and remediate identified risks and implement security measures. Create and deploy methodologies, templates, guidelines, checklists, procedures, and other documents in support of the court's IT security framework.
- Develop, analyze, and evaluate new and innovative information technology policies that

will constructively transform the information security posture of the court units. 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 are 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.
- Manage information security projects (or security-related aspects of other projects) to ensure milestones are completed in the appropriate order and on schedule. Prepare special management reports for the court unit(s), as needed.
- Establish mechanisms to promote awareness and adoption of security best practices.
- Develop policies and procedures to ensure information systems' reliability and to prevent and defend against unauthorized access to systems, networks, and data.

Minimum Qualifications/Requirements

- To qualify at the CL 28 level, the applicant must have two years specialized experience, including at least one year equivalent to work at the next lower grade (CL 27). To qualify for this position at the CL 29 level, the applicant must have three years specialized experience, including at least one year equivalent to work at the next lower grade (CL 28).
- Strong understanding of IT security best practices and demonstrated ability to analyze, design and implement, and train security procedures.
- Excellent written and oral communication, presentation, organizational and interpersonal skills.
- Strong troubleshooting abilities and customer service skills are mandatory. The employee must be able to occasionally work after hours and weekends. Some travel, including overnight trips, will be required. Occasional lifting may be required.

Preferred Qualifications

- Bachelor's Degree in Computer Science or related field.
- CISSP, CompTIA Security+ training or certification.
- Experience with Tenable Security Center, Nessus Vulnerability Scanner, Splunk Log Management, Symantec Endpoint Protection, Malwarebytes, KACE Patch Management, PDQ Inventory and Deploy, Forcepoint Web Security, AirWatch/Workspace One MDM, Palo Alto firewalls.
- Preference will be given to those candidates who possess significant professional IT security experience, and strong understanding of IT security best practices, and demonstrated ability to analyze, design, and implement security practices and procedures. Knowledge and expertise in theories, principles, practices, and techniques of network management and security, enterprise level IP firewalls, IT networks, network traffic.

Benefits

- Ten (10) paid federal holidays
- Paid annual and sick leave
- Retirement benefits under the Federal Employees Retirement System
- Optional participation in the Thrift Savings Plan (similar to a 401(k)), with matching employer contributions
- Optional Health Benefits Program, Dental and Vision insurance, Group Life Insurance, and Long Term Care insurance
- Flexible Benefits Program

Applicant Information

- Only qualified applicants will be considered for this position. Employees of the U.S. Courts serve under "Excepted Appointments" and are considered "at will" employees. Federal Civil Service classifications or regulations do not apply; however, court employees are entitled to substantially the same benefits as other Federal Government employees. Judiciary employees must adhere to the Code *of Conduct for Judicial Employees.*
- Applicants are advised that false statements or omissions of information on any application materials may be ground for non-selection, or withdrawal of an offer of employment, or dismissal after being employed.
- Participation in the interview process will be at the applicant's own expense and relocation expenses will not be provided.
- As a condition of employment, the selected candidate must successfully complete a ten-year background investigation with periodic updates every five years thereafter.
- Applicant must be a U.S. citizen or be eligible to work in the United States. Non-citizens may be interviewed and considered for employment, but employment offers will only be made to individuals who qualify under one of the exceptions in 8 U.S.C. Section 1324b(a)(3)(B). Non-citizens who have not been permanent residents for five years will be required to execute an affidavit that they intend to apply for citizenship when they become eligible to do so.
- All appointments subject to mandatory electronic funds transfer for payment of net pay.

Application Process

Qualified applicants must submit an application package in PDF format including:

- A cover letter
- A complete AO 78 Application for Judicial Employment (available on the court's "Job" page)
- A current resume
- A list of three professional references

Submit application materials to:

Caeb_HR@caeb.uscourts.gov

- Application packages lacking any of the requirements or are not in the correct format will not be considered.

The Court reserves the right to modify the conditions of this job announcement or to withdraw the announcement, either of which may occur without prior written or other notice. The United States Bankruptcy Court is an Equal Employment Opportunity employer.