



MARK B. BUSBY
Clerk of Court

San Francisco Division
450 Golden Gate Avenue
San Francisco, CA 94102

Oakland Division
1301 Clay Street
Oakland, CA 94612

San Jose Division
280 South 1st Street, Room 2112
San Jose, CA 95113

**Eureka-McKinleyville
Division**
3140 Boeing Avenue
McKinleyville, CA 95519

CAND MISSION

The mission of the Clerk's Office of the United States District Court for the Northern District of California is to support, defend and preserve the Constitution of the United States by:

- Serving and supporting the court
- Providing access to the court
- Maintaining the records of the court
- Providing information about the court
- Performing our mission with a commitment to excellence

*The United States District Court is
an Equal Focused Employer*

CAREER OPPORTUNITY

UNITED STATES DISTRICT COURT NORTHERN DISTRICT OF CALIFORNIA

Position: IT Security Officer

Classification Level: CL28/CL29

Salary Range CL28: \$86,573 - \$140,753; CL29: \$102,962 - \$167,349 (DOE)

Pay Tables by location: [CPS Pay Rates \(non-law enforcement officer\)](#)

Location: Full-time Telework or San Francisco, CA

Opening Date: December 3, 2024

Closing Date: Open Until Filled

(Priority consideration to applicants who apply by December 20, 2024)

Whether launching or continuing a career in public service, the U.S. District Court is a great place to work with competitive salaries and benefits, a work schedule that promotes a work-life balance, access to a fitness center, and the opportunity to work with colleagues committed to fulfilling the important mission of administering justice in an efficient and effective manner. This position offers an excellent opportunity to advance a career in Federal court service.

POSITION OVERVIEW

The Northern District of California District Court, Probation Office, and Pretrial Services Agency, seek a talented IT Security Officer, a professional who loves to pro-actively advance security priorities and engage customers in security awareness, training, and best practices. The district is looking for a self-starter who will improve the district's security posture and collaborate with other regional and national judiciary stake holders. As part of several information technology teams, you will work in a professional work environment to deliver impactful security initiatives for the United States Judiciary and have the opportunity to support nationwide programs. Secondary responsibilities include assisting the network administrators in the administration of the judiciary's information technology network by developing standards, recommending network infrastructure change, and participating in the high-level and long-term design and analysis of the courts' network systems.

REPRESENTATIVE DUTIES:

- Review, evaluate, and make recommendations on courts' 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 track, triage, and remediate identified security risks and implement security measures. Coordinate the remediation of larger security risks with other IT team members and advise management when additional resources are needed.
- 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 to system vulnerabilities and monitor for outdated applications and security-related matters.

- Communicate and provide advice on matters of IT security, including security strategy and implementation to judges, court unit executives, and other court staff managers.
- Assist in the development and maintenance of local court unit security policies and guidance. Serve as a resource to all court units within the district regarding federal and judiciary 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.
- Establish mechanisms to promote security. Train court staff on security awareness and adoption of security best practices.
- Serve as a team lead 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 the primary contact for external security assessments and audits, and address relevant issues found.
- Perform analysis, remediation, forensics, and any other activities need concerning any IT security incidents.
- Coordinate with local IT staff and the judiciary Security Operations Center to resolve issues and take any required action, immediate or otherwise.
- Work hours are regular business hours, Pacific Time, but the position requires on-call availability. A mobile phone is provided.

QUALIFICATIONS

Minimum Qualifications

To qualify at the CL 28 level, the applicant must have two years of specialized experience, including at least one year equivalent to work at the next lower level (CL 27). To qualify for this position at the CL 29 level, the applicant must have three years of specialized experience, including at least one year equivalent to work at the next lower level (CL 28).

Specialized experience is progressively responsible experience that is in, or closely related to, the work of the position that has provided the knowledge, skills, and abilities to successfully perform the duties of the position.

- Experience with IT security tools and the ability to learn new tools and methods.
- System administration experience.
- Ability to perform independent research and identify training needs.
- Ability to collaborate with individuals, teams of any size, and organizations of any size.
- The ability to work with other local and remote technical staff to identify, prioritize, and resolve security issues - especially those identified in security scans.
- Good judgment, be dependable, be a proactive self-starter, and demonstrate initiative in problem-solving.
- Exceptional ability to effectively communicate, articulate, and relate to coworkers and others with professionalism and integrity.

Preferred Qualifications

- Experience with IT security tools used by the US Courts (Splunk, Nessus, KACE,

Forcepoint, KnowBe4, Apex One, Deep Security (Trend Micro), Palo Alto (JFS), VMware VRA8 and CIS Critical Security Controls v8).

- Experience in, or with, the US Courts, government or large organizations.
- Ability to create and maintain policies, end-user documentation, and instructions.
- Ability to perform internal IT security assessments and self-audits, and monitor policy adherence, understanding of CIS Critical Security Controls v8 (Center of Internet Security).

COMPENSATION AND BENEFITS

Compensation will be set based on experience and qualifications pursuant to the policies and guidelines set forth in the Court Personnel System (CPS). Employees qualify for retirement plans, federal employee's group health insurance, life insurance, dental/vision insurances, and flexible benefits. For more information about federal court benefits, please visit:

www.uscourts.gov/careers/benefits.

INFORMATION FOR APPLICANTS

The successful candidate for this position is subject to a FBI fingerprint check and background investigation (employment will be provisional and contingent upon the satisfactory completion of the required background investigation), must adhere to a [code of conduct](#), and must arrange for direct deposit of federal wages. Travel expenses for interviews or relocations are not available. The Court reserves the right to modify the conditions of this job announcement, or to withdraw the announcement without prior written or other notice.

Non-citizens may be interviewed and considered for employment, but employment offers will only be made to individuals qualifying under one of the exceptions in 8 U.S.C. § 1324b(a)(3)(B). In most cases, an offer of employment cannot be made unless the candidate is a lawful permanent resident who is seeking U.S. citizenship. Contact Human Resources at 415-522-2147 for more information.

Equal Focused Employer

We value diversity and are committed to equity and inclusion in our workplace. The Court encourages applications from all qualified individuals and seeks a diverse pool of applicants in terms of race, ethnicity, national origin, sex, gender identity and expression, sexual orientation, age, languages spoken, veteran's status, disability, religion, and socio-economic circumstance.

The court provides reasonable accommodation to applicants with disabilities. Notify Human Resources at 415-522-2147 to request a reasonable accommodation for any part of the application or hiring process. Human Resources will determine requests on a case-by-case basis.

APPLICATION PROCEDURE

To apply, complete the online application at www.governmentjobs.com/careers/uscourtsand and upload a resume and cover letter in Word or PDF format where requested.