Position Announcement 24-05
NATIONAL INFORMATION TECHNOLOGY OPERATIONS AND APPLICATIONS DEVELOPMENT
IT SECURITY MANAGER
Office of the Federal Public Defender
Western District of Texas (**SAN ANTONIO**)

THE FEDERAL PUBLIC DEFENDER, Western District of Texas is accepting applications for the position of IT Security Manager, National Information Technology Operations and Applications Development (NITOAD), in San Antonio, Texas. The NITOAD branch supports the federal defender program's staffed offices in 204 locations throughout the continental United States, Alaska, Hawaii, Puerto Rico, the Virgin Islands, and Guam. The federal defender program operates under authority of the Criminal Justice Act, 18 U.S.C. § 3006A, to provide defense services in federal criminal cases and related matters by appointment from the court to individuals unable to afford counsel.

Job Requirements. To qualify for the NITOAD Branch IT Security Manager position, a person must be a high school graduate or equivalent, however a bachelor's degree is preferred. The candidate must also have at least three years of general experience and five years of specialized experience with network and system administration principles, practices, methods, and techniques. Some higher education from an accredited college or university, preferably with a concentration in computer or management-information science or a related field, may be substituted for some of the required experience. Regardless of educational substitution, candidates must have specialized experience in two or more of the following areas:

- The ability to maintain technical competency by reading, analyzing, and interpreting common technical journals and documents;
- Proficiency in understanding, adhering to, and implementing federal IT policies and regulations to include FISMA and NIST;
- The ability to recognize and analyze security deficiencies and recommend a corrective plan of action;
- High level of business acumen, strategic agility, ability to develop others, and influence outcomes and change (key results);
- Excellent interpersonal, written, and oral communication skills, especially being able to communicate with different groups of people, from end users with little technical knowledge to senior staff.

The ability to lift 50 pounds and occasional travel, including overnight travel, is required. A candidate must have a general understanding of office confidentiality issues, such as attorney/client privileges. Experience with a public defender, law office, or court functions policies and procedures are preferred. The selected candidate must complete a ten-year background investigation with periodic updates every five years thereafter. Employment will be considered provisional pending the initial ten-year background investigation. Continued employment will depend upon favorable determinations from the background investigation. Applicants must be US citizens or be authorized to be employed by the federal government. The full position qualifications statement with position description is available upon request.

Duties. The IT Security Manager plays a critical role in overseeing the information security program for the Federal Defender system. Responsibilities include ensuring compliance with Judiciary guidelines, developing, and overseeing NITOAD security initiatives and safeguarding sensitive client and case-related information. This role involves supervising security teams and serving as the escalation point for critical issues. Additionally, the IT Security Manager acts as a subject matter expert on IT security and provides advice to upper management. The focus is on proactive measures, staying ahead of cyber threats, and maintaining a vigilant stance in safeguarding the organization's digital assets. The IT Security Manager performs and supervises the performance of tasks such as the following:

- Administers proactive security programs to identify and minimize deficiencies across the Federal Defender organization (FDO).
- Reviews proposed systems, networks, and software designs for potential security risks; recommends countermeasures, ensuring seamless integration with existing infrastructure.
- Coordinates regular security posture assessments for both internal and external networks.
- Oversees vulnerability assessments and penetration testing activities to stay ahead of emerging threats.
- Directs the efforts of the Security Operations Center (SOC) to swiftly identify, investigate, and resolve issues affecting the security of FDO information assets.
- Leads cybersecurity incident response efforts, ensuring a rapid and effective response to any security breaches.
- Exercises supervisory skills in directing subordinate staff, providing valuable feedback on their work product.
- Develops long-range plans for IT security systems that anticipate, identify, evaluate, and mitigate risks associated with system vulnerabilities.
- Prepares and presents insightful briefings to senior management officials on complex IT security issues, fostering understanding and informed decision-making.
- Plays a key role in the development of policies, procedures, and guidelines related to FDO IT security issues.
- Identifies and selects cutting-edge IT security training materials and collaborates with NITOAD management to coordinate and conduct training programs for all levels of staff throughout the FDO.
- Establishes effective mechanisms to promote awareness and adoption of security best practices, ensuring a culture of security consciousness.
- Leads the implementation and support of projects within a defined timeline, budget, and scope constraints; showcasing expertise in navigating complex IT landscapes.

Salary and Benefits. The starting salary will be commensurate with the experience and qualifications of the applicant within a range of $104,887 (JSP-13, Step 1) to $123,945 (JSP-14, Step 1) per annum. The position is in the excepted service and does not carry the tenure rights of the competitive Civil Service. The position does offer federal government employee benefits, including health and life insurance programs, retirement, and the Thrift Savings Plan. Salary is payable only by Electronic Funds Transfer (direct deposit).

How to Apply. Qualified persons may apply by submitting a letter of interest (mentioning announcement number 24-05), a résumé, and three professional references to: Maureen Scott Franco, Federal Public Defender, Western District of Texas, 8200 West Interstate 10, Suite 1000, San Antonio, Texas 78230, or you may submit the required documents in a single PDF document named with applicant's "last name, first name-Announcement 24-05 IT Security Manager" by email to NITOAD_Admin@fd.org. You may also apply by submitting your application via Indeed.com. Electronic submissions sent directly to the Defender will not be considered. For applicants with disabilities, this organization provides reasonable accommodations, which are decided on a case-by-case basis. To request a reasonable accommodation for any part of the application or interview process, contact personnel administrator Victoria B. Longoria at (210) 981-2081. Position announced January 20, 2024, subject to the availability of funds; open until filled.

The Federal Public Defender is an equal-opportunity employer.