DISTRICT OF NEW HAMPSHIRE
UNITED STATES DISTRICT COURT
BANKRUPTCY COURT
PROBATION & PRETRIAL SERVICES
CONCORD, NEW HAMPSHIRE 03301

IT SECURITY OFFICER (2021-01B)

Location	Concord, NH
Salary Range	CPS CL28 $69,023 to $112,172
Closing Date	January 7, 2022

Position Description

The IT Security Officer primarily performs professional work related to the management of information technology security policy, planning, development, implementation, training, and support for the court. The incumbent provides IT security and serves as a team lead to fulfill security objectives within the court. The incumbent ensures the confidentiality, integrity, and availability of systems, networks, and data and creates, promotes, and adheres to standardized/repeatable processes for the delivery of security services. The IT Security Officer proactively engages all users in security awareness and training activities to promote the appropriate use of best security practices. The incumbent is responsible for assisting in the implementation of local security policies, processes, and technologies that are consistent with the national information security program as well as for collaborating with other judiciary stake holders, such as the Administrative Office and other court IT personnel, to identify and collectively advance security initiatives both within and beyond court unit boundaries. Other responsibilities include assisting the network administrator in the administration of the judiciary's information technology network by developing standards, recommending network infrastructure change, and participating in high-level and long-term design and analysis of the court's network systems. The incumbent will also work with endpoint administrators to ensure the secure deployment of devices into production.

Primary Representative Duties

- Review, evaluate, recommend, and enact change to the district's technology security programs. Promote and provide support of existing information security services, including those that are pertinent to network infrastructure, locally developed and nationally supported software applications, software, data, voice, and video telecommunications, mobile/remote access, and other technologies used by the court.
- Provide technical advisory and remediation recommendations and best practices to securely design, implement, maintain, or modify IT systems and networks. Perform research, implement and maintain audits, and perform security vulnerability scanning to identify potential vulnerabilities in, and threats to, existing and proposed technologies, and notify the appropriate personnel of the risk potential. Recommend changes to ensure the reliability of information systems and to prevent and defend against unauthorized access to systems, networks, and data.
- Partners with the Director of Information Technology to serve as the IT security incident response team leader. Coordinates security efforts with other members of the IT security incident response team. Facilitates appropriate action and response to various information security incidents. Logs, tracks, documents, communicates security activity through the lifecycle of the incident.
- Serves as a first level approver for all IT security exceptions. Once approved, the ITSO will maintain a comprehensive list, routinely assessing methods to remove the exception.

- Provide technical advisory services on matters of IT security, including security strategy and implementation, to court executives, and other senior court staff. Educate project stakeholders about security concepts. Create and employ methodologies, templates, guidelines, checklists, procedures, and other documents to establish repeatable processes across the court's information technology security services.
- Assist in the development and maintenance of local court unit security policies and guidance, the remediation of identified risks, and the implementation of security measures.
- Provide security analysis of IT activities to ensure that appropriate security measures are in place, documented and enforced. Conduct security risk and vulnerability assessments of planned and installed information systems to identify weaknesses, risks, and protection requirements.
- Manage information security projects (or security-related aspects of other IT projects) to ensure milestones are completed in the appropriate order and according to schedule. Prepare special management reports for the court as needed.
- Perform routine scans and remediations to system vulnerabilities and monitor for outdated applications and security related matters.
- Serve as 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.
- Promote awareness and adoption of security best practices based on the Administrative Office Guidelines and security practices. Supply court staff with routine security tips, as well comprehensive security training annually.
- Serve as a liaison with court stake holders to integrate security into the system development lifecycle.

Secondary Representative Duties (May Include Backup to Network Administrator)

- Install and maintain server operating systems, infrastructure equipment, and applicable software to manage network infrastructure.
- Network and server support (LAN and WAN access), including routers and switches.
- Create and monitor user accounts, assign passwords and provide security training as needed.
- Monitor and assure backup routines are successful and operating as expected. Assist in disaster recovery operations and testing, including network performance, web usage/monitoring and design.
- Monitor, maintain and resolve issues related to the court's SAN and converged media appliance.
- Maintain wireless network within the courthouse.
- Assist in managing Active Directory.

Qualifications

- Five years of professional IT security experience is preferred. Experience may include:
    - Extensive knowledge of IT systems and network security, network traffic analysis, computer hardware and software, and data communications.
    - Creation of IT security awareness training programs for users and IT staff.
    - Ability to identify and analyze security risks and implement resolutions.
    - Knowledge of anti-virus, anti-malware, application control, web threat protection and endpoint security controls. Knowledge of and experience with enterprise-level firewalls (Cisco ASA / Palo Alto). Understanding of incident response processes, including the ability to implement plans and procedures.
- A bachelor's degree or higher in the information technology field from an accredited institution is preferred.
- Any of the following certifications are highly desired:
    - CompTIA Security+

  - CompTIA PenTest+
  - CompTIA Cybersecurity Analyst (CySA+)
  - CompTIA Advanced Security Practitioner (CASP+)
  - Certified Information Security Manager (CISM)
  - Certified Information Systems Security Professional (CISSP)
  - SANS GIAC Security Essentials (GSEC)
  - Certified Ethical Hacker (CEH)
  - Offensive Security Certified Professional (OSCP)
  - Certified Cloud Security Professional (CCSP)

- Skill in interpersonal communications, including the ability to use tact and diplomacy in dealing effectively with all levels of management, staff, and judicial officers.
- Skill in project management, organizing information, managing time, and balancing multiple work assignments effectively, including prioritizing and meeting tight deadlines.
- Self-motivated, detail-oriented and organized.
- Ability to manage multiple priorities and problem solve under pressure.
- Must possess excellent verbal and written communication skills.
- Must present a professional demeanor, positive personality, and work well in a team environment.
- Applicants must be U.S. Citizens or meet the exceptions to the statutory restriction on origin non-citizens to work in the federal government in the continental United States.

Additional Information

The Federal Financial Management Reform Act requires direct deposit of federal wages. As a condition of employment, the selected applicant will be subject to a background investigation by law enforcement agencies and may be required to provide educational transcripts. The selected candidate will be hired provisionally pending successful completion of the background investigation and a favorable suitability determination. Unsatisfactory findings may result in termination of employment. Judiciary employees serve under excepted appointments and are considered "At Will" employees. Some travel may be required.

How To Apply

Qualified applicants should submit a letter of interest, a resume, and a salary history for the past ten years in one PDF document to Thomas Van Beaver at

tom_vanbeaver@nhd.uscourts.gov

by the close of business on **January 7, 2022**. The applicants deemed most qualified will be invited to participate in a personal interview at their own expense. References will not be required until an applicant is considered a finalist. The Clerk of Court reserves the right to modify the conditions of this vacancy announcement at any time or to withdraw it without prior notice.

The District of New Hampshire is an equal opportunity employer.