

**UNITED STATES DISTRICT  
COURT FOR THE  
DISTRICT OF WYOMING**



**Announcement No.:** 2023-06

**Position Location:** Cheyenne, WY

**Position Information:**

*Full-time, permanent, Excepted  
Service*

**Area of Consideration:**

*Open to all qualified sources*

**Open Date:** November 21, 2023

**Closing Date:** Preference will be  
given to applications received by  
December 22, 2023

**Our Mission:**

*Employees representing the U.S. District  
Court for the District of Wyoming are com-  
mitted to the impartial administration of jus-  
tice. Driven by respect, integrity, and a dedi-  
cation to excellence, we are here to serve the  
Public, Bar, and Court in a manner that will  
instill trust and confidence in the Judiciary.  
We endeavor to support a just and timely  
resolution of matters brought before the  
Court.*



**NOTICE OF POSITION VACANCY**

**Position Title:** IT Security Officer

**Grade/Salary Range:** CL 28, Step 1 - CL 28, Step 61  
(\$66,250 - \$107,701)

- Salary dependent on experience and qualifications

**How to Apply:**

Applicants will be required to submit the following:

- 1) AO-78, Federal Judicial Branch Application for Employment (which can be found on the US Courts website at: <https://www.uscourts.gov/forms/human-resources-forms/application-judicial-branch-federal-employment>)
- 2) Cover letter
- 3) Resume (including day and evening telephone numbers)

Applications can be submitted electronically via email in  
ONE PDF to: [hr@wyd.uscourts.gov](mailto:hr@wyd.uscourts.gov)

Only applicants selected for an interview will be notified. In-  
complete applications will not be considered.

---

## **POSITION SUMMARY**

The IT Security Officer performs professional work related to the management of information technology security policy, planning, development, implementation, training, and support for the District Court, Probation and Bankruptcy Court. The incumbent provides actionable advice to improve IT security and serves as a team lead to fulfill security objectives within the District. The incumbent ensures the confidentiality, integrity, and availability of systems, networks, and data across the system development life cycle (SDLC), and creates, promotes, and adheres to standardized, repeatable processes for the delivery of security services. The IT Security Officer pro-actively engages all users in security awareness and training activities to promote the appropriate use of best security practices within the District. The incumbent is responsible for implementing 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 the District's boundaries. The IT Security Officer will report to the District Court's Chief Deputy.

---

## **SUMMARY OF REPRESENTATIVE DUTIES AND RESPONSIBILITIES**

- 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 local court unit.
- 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 local court unit. Perform research to identify potential vulnerabilities in, and threats to, existing and proposed technologies, and notify the appropriate managers/personnel of the risk potential.
- Provide advice on matters of IT security, including security strategy and implementation, to judges, court unit executives, and other senior court unit staff.
- 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.
- Develop, analyze, and evaluate new and innovative information technology policies that will constructively transform the information security posture of the court unit. 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.
- Assist with the identification, implementation, and documentation of security safeguards on information systems. Manage information security projects (or security-related aspects of other IT projects) to ensure milestones are completed in the appropriate order, in a timely manner, and according to schedule. Prepare justifications for budget requests. Prepare special management reports for the court unit, as needed.

- Serve as a liaison with court stakeholders to integrate security into the system development lifecycle. Educate project stakeholders about security concepts, and create supporting methodologies and templates to meet security requirements and controls.
  - Recommend changes to ensure information systems' reliability and to prevent and defend against unauthorized access to systems, networks, and data.
  - Create and employ methodologies, templates, guidelines, checklists, procedures, and other documents to establish repeatable processes across the courts' information technology security services.
  - Establish mechanisms to promote awareness and adoption of security best practices.
- 

## **QUALIFICATIONS**

- To qualify at the CL 28 level, the applicant must have a minimum two years of relevant security experience, including at least one-year equivalent to work at the next lower level (CL 27).
- Experience with IT security tools and the ability to learn new tools and methods.
- Experience with System administration, including current Microsoft server and workstation operating systems, networking fundamentals, and troubleshooting techniques
- 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 co-workers and others with professionalism and integrity.

## **PREFERRED QUALIFICATIONS:**

- Experience with IT security tools used by the US Courts: Splunk, Nessus, KACE, Forcepoint, Trend Micro Apex One and Deep Security.
- 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.

---

## **BENEFITS**

Full-time employees of the United States District Court for the District of Wyoming are eligible for a full range of benefits to include:

- A minimum of 11 paid holidays per year
- Paid annual leave in the amount of 13 days per year for the first three years, 20 days per year after three years, and 26 days per year after fifteen years
- Paid sick leave in the amount of 13 days per year
- Federal Employees' Retirement System (FERS)
- Optional participation in the Thrift Savings Plan (TSP), the Federal Employees Health Benefits Program (FEHBP), Federal Dental and Vision Insurance Program (FEDVIP), the Federal Employees' Group Life Insurance (FEGLI), the Flexible Benefits Program
- Federal Occupational Health Services Program (FOH)
- Employee Assistance Program (EAP)/Work Life Services
- Virtual Learning through the Judiciary Online University
- Student Loan Forgiveness for Public Service Employees

*For more detailed information about Federal Judiciary benefits, please visit [www.uscourts.gov/careers/benefits](http://www.uscourts.gov/careers/benefits).*

---

## **CONDITIONS OF EMPLOYMENT**

Applicants must be U.S. citizens or eligible to work in the United States.

This position is subject to mandatory electronic funds transfer (direct deposit) for salary payment. Appointment is provisional and contingent upon successful completion of a favorable suitability determination, reference check, and background check and fingerprinting.

Judiciary employees serve under excepted appointments and are considered "at will" and can be terminated with or without cause by the Court. Employees are required to adhere to the Code of Conduct for Judicial Employees and court confidentiality requirements. Appointee may be removed from this position for failure to perform at a satisfactory level following reasonable on-the-job training.

The Court is not authorized to reimburse candidates for travel or moving expenses.

The Court reserves the right to modify, withdraw, or fill the vacancy announcement at any time, any of which actions may occur without prior written or other notice.

**THE UNITED STATES DISTRICT COURT IS AN  
EQUAL OPPORTUNITY EMPLOYER**