



# Administrative Office of the Courts

## Job Description

<b>Job Title:</b>	AOC IT Security Architect	<b>Grade:</b>	IT10
<b>Division:</b>	Court Information Systems	<b>Revision Date:</b>	May 26, 2023

### POSITION SUMMARY:

The Administrative Office of the Courts (AOC) is an agency within the judicial branch of government that works to support the state courts on behalf of the Arkansas Supreme Court. The Court Information Systems Division (CIS) is responsible for providing technological support to the state's courts, making court information available to the public, and developing and implementing online, court-related services. CIS is a team-based organization using the Disciplined Agile framework. You may view our Statement of Core Values at <https://www.arcourts.gov/modernization/statement-core-values>.

The AOC Information Technology Security Architect is responsible for architecting security for the systems and services provided by the Court Information Systems Division for the Arkansas Supreme Court, Court of Appeals, Administrative Office of the Courts, and other entities within the Judicial Branch. The position is responsible for implementing IT security policies and monitoring compliance with adopted policies through system auditing. The IT Security Architect is a member of the network and security team and is required to work closely with the AOC Chief IT Security Officer and the CIS Leadership team to support technology security initiatives for projects and operational activities.

### JOB DUTIES:

- Oversee the security integrations for the systems in the Amazon Web Services (AWS) government cloud.
- Design and implement automated processes that enhance security and improve efficiency in AOC Cloud environments.
- Assist the AOC in monitoring database and server logs, firewall logs, IPS logs and network traffic for unusual or suspicious activity with an emphasis on AOC Cloud operations.
- Configure and monitor system security devices.
- Assist the AOC in deploying, managing, and maintaining system security infrastructure with emphasis on AWS Government Cloud.
- Implement incident response actions.
- Assist with the development, implementation, maintenance and enforcement of security policies, procedures, and associated plans for system security administration and user system access.
- Assist with the maintenance of policy and procedure documentation and prepare reports.
- Assist with the education for end user security awareness.
- Stay current with emerging security alerts and issues.
- Conduct active penetration tests to discover vulnerabilities in information systems.
- Participate in DR/COOP planning and testing.
- Other duties as assigned.

### QUALIFICATIONS:

- **Education**
  - The Information Technology Security Analyst must have a bachelor's degree in computer science or a related field with emphasis in IT security.
  - Relevant IT security and networking certifications (CCNA, CCNP, CISSP, SSCP, GIAC, CISM, Security+, CEH, LPT, Q/ISP, AWS Certified Security - Specialty) are highly desirable.
- **Experience**
  - Two years of experience in the use of security auditing and monitoring systems such as LogRhythm, Rancid, Nessus, ElasticSearch, Graylog and Wireshark are preferred.
- **Knowledge, Skills, Abilities**
  - Knowledge of information technology security best practices.
  - Knowledge of .NET Core and the Entity Framework Core.

**Applicants should send their resume, contact information and contact information for three professional references to [Cecil.davis@arcourts.gov](mailto:Cecil.davis@arcourts.gov)**

- Knowledge of Amazon, Oracle, and Microsoft cloud services..
- Knowledge of information technology security solutions, including hardware and database management practices to secure information.
- Ability to architect security and support security testing for web applications.
- Ability to design and build open-source security systems.
- Ability to assess IT security needs for projects and processes.
- Ability to work well independently and as part of a team.
- Ability to coordinate activities with court staff, users, and vendor representatives.
- Ability to communicate effectively, orally and in writing.
- Ability to analyze problems and make effective recommendations and decisions.
- Ability to communicate complex technical subjects clearly and concisely.

Last Updated By:	
------------------	--