

POSITION ANNOUNCEMENT – 26-43

Assistant Computer Systems Administrator (ACSA) – IT Network Administrator

Office of the Federal Public Defender

District of Arizona

Phoenix

THE FEDERAL PUBLIC DEFENDER for the District of Arizona is accepting applications for the position of a full-time Assistant Computer Systems Administrator (ACSA) – IT Network Administrator to be stationed in Phoenix, Arizona. The Federal Public Defender operates under authority of Title 18, United States Code, Section 3006A(g)(2)(A), to provide federal criminal defense services by court appointment to individuals unable to afford counsel. The Federal Public Defender, District of Arizona has offices in Phoenix, Tucson, Yuma, and Flagstaff.

Overview

We are seeking a skilled and customer-focused Assistant Computer Systems Administrator (ACSA)- IT Network Administrator. The Assistant Computer Systems Administrator (ACSA) - IT Network Administrator is primarily responsible for the administration, security, reliability, and performance of the organization's enterprise network and infrastructure environment. This is a hands-on position requiring strong experience in network administration, Windows server infrastructure, virtualization, storage, and cybersecurity operations across multiple locations.

Key Responsibilities

- Configure, administer, monitor, and troubleshoot enterprise network infrastructure — switches, firewalls, wireless, TCP/IP, VLANs, routing, DNS/DHCP, and segmentation.
- Administer Windows Server infrastructure, Active Directory, Group Policy, and related Microsoft technologies; support virtualization environments (VMware vSphere and/or Hyper-V).
- Support physical and virtual server infrastructure and enterprise storage (SAN, NAS, iSCSI, CIFS/SMB), including hardware installation, upgrades, and lifecycle management.
- Administer backup and recovery infrastructure (preferably Veeam); monitor operations, investigate failures, and support disaster-recovery and business-continuity activities.
- Support cybersecurity operations — secure configuration, vulnerability remediation, patch management, access control, and incident investigation/remediation.
- Maintain physical data room/data center infrastructure (racking, cabling, power, environmental conditions) and perform hardware inspections and replacements.
- Assist with design, deployment, and security of on-premises AI infrastructure, including network segmentation, access controls, and monitoring for internal AI systems.
- Maintain accurate network diagrams, documentation, and inventories; develop scripts/automation to improve infrastructure operations.
- Research and evaluate emerging technologies in networking, cybersecurity, virtualization, and AI, and support infrastructure projects and upgrades.
- Provide secondary support for Windows 11 workstations, VPN/endpoint security, and mobile devices (Android, iPhone, iPad), plus backup support to other IT functions as needed.

Required Qualifications

- A high school diploma or equivalent is required. A bachelor's degree in computer science, information technology, cybersecurity, or a related field, along with relevant technical certifications (e.g., CompTIA Network+/Security+) is preferred. Candidates must have at least three years of specialized IT support experience.
- Demonstrated experience with enterprise network administration and troubleshooting. (switches, routers, firewalls, VPNs, TCP/IP, VLANs, segmentation).
- Strong working knowledge of Windows Server, Active Directory, DNS, DHCP, and Group Policy.
- Experience with VMware vSphere and/or Microsoft Hyper-V and supporting enterprise server/network/data center operations, including performance and capacity monitoring.
- Working knowledge of network storage (SAN, NAS, iSCSI, CIFS/SMB) and enterprise backup/recovery technologies (preferably Veeam).
- Experience with enterprise server, network, and/or data center operations to include monitoring server performance, availability, and troubleshoot infrastructure issues.
- Support physical data room operations, including equipment installation, server rack and cable management, hardware inspection, equipment maintenance, and troubleshooting.
- Knowledge of cybersecurity fundamentals, including vulnerability remediation, patch management, network security, and secure infrastructure configuration.

- Assist with hardware installation, replacement, upgrades, and infrastructure lifecycle management.
- Strong troubleshooting, analytical, organizational, and problem-solving skills.
- Ability to work independently and collaboratively in a multi-site IT environment.
- Strong written and verbal communication skills and the ability to communicate effectively with technical and non-technical audiences.
- Research, test, and evaluate emerging technologies in networking, cybersecurity, virtualization, infrastructure, and AI.
- Commitment to maintaining accurate and current technical documentation.
- Ability to lift up to 50 pounds on a frequent basis and work occasionally in the evenings, weekends, or after-hours maintenance windows.

Preferred Qualifications

- Experience with enterprise firewall, VPN, and network-monitoring technologies.
- Experience with high-availability infrastructure and disaster recovery, business continuity, and supporting multi-site/WAN environments.
- Experience with PowerShell, or other scripting and automation technologies.
- Familiarity with on-premises AI infrastructure, GPU-enabled systems, or secure AI workloads.
- Knowledge of AI tools is a plus: machine learning concepts, automation, AI-assisted workflows, and services leveraging AI specific workflows and applications, such as: Docker, vLLM, WhisperX, ollama, OpenWebUI, RAG, LLMs, etc.

This position works under the direction of the Supervisory Computer Systems Administrator and assists with supporting and maintaining the organization's Microsoft Windows network infrastructure in a wide area network (WAN) environment. This position may require occasional travel, weekend work, and the performance of other duties as assigned.

Employment is subject to a satisfactory background investigation. All claimed experience, certifications, training, and references will be checked. U.S. Citizenship is required.

Salary and Benefits. The starting salary for the ACSA positions will be set commensurate with the experience and qualifications of the applicant starting at Grade 11, Step 1 yielding \$78,117, through Grade 12, Step 10 yielding \$121,720. These positions are in the excepted service and do not carry the tenure rights of the competitive Civil Service. The positions do include regular government employee benefits including health and life insurance, retirement, and the Thrift Savings Plan. Salary is payable only by Electronic Funds Transfer (direct deposit). Offer of employment is subject to the availability of funds.

How to Apply. Qualified persons should apply via the online application system at <https://azfd.acquiretm.com/home.aspx>. To be considered for the position, applicants need to register at the above web address and create an online profile, or login if you already have a profile. Please follow the prompts to upload a letter of interest, résumé, and three professional references. Position announced 09/16/2026; Closes; Open until filled.

The Federal Public Defender is an equal-opportunity employer. All applicants, regardless of race, ethnicity, national origin, gender identity, sexual orientation, religion, disability, or age, are encouraged to apply.