



**POSITION ANNOUNCEMENT 27-02**  
**NATIONAL INFORMATION TECH OPERATIONS AND APPLICATIONS DEVELOPMENT**  
**IDENTITY AND ACCESS ADMINISTRATOR**  
Office of the Federal Public Defender  
Western District of Texas

**Position:** Identity and Access Administrator  
**Location:** San Antonio, Texas  
**Salary:** \$90,823 - \$108,001

**Position Type:** Full-Time  
**Opening Date:** October 15, 2026  
**Closing Date:** Until Filled

The Federal Public Defender for the Western District of Texas is accepting applications for the position Identity and Access Administrator, to be stationed in the San Antonio office.

#### **POSITION DUTIES**

The Identity and Access Administrator's role involves executing and optimizing a cloud identity ecosystem that aligns with the organization's goals to ensure the security, reliability, and scalability of NITOAD's hybrid-cloud environment. The duties of an Identity and Access Administrator duties include:

- Administers and manages end-user identity lifecycle across on-premises Active Directory (AD) and Microsoft Entra ID hybrid environment.
- Manage Enterprise AD servers, including physical and virtual domain controllers, replication health, patching, backups, and service availability.
- Monitor identity security posture and remediate risks which include risky sign-ins, compromised accounts, behavior anomalies, and stale objects.
- Enterprise Privilege Access Management (PAM) and third-party AD management tools administration.
- Configure Entra conditional access policies, MFA, privileged identity management, and identity protection controls.
- Provides Tier-3 support assisting IT staff around the nation with in-depth technical support and troubleshooting advanced problems.
- Develop and maintain documentation such as: infrastructure diagrams, installation documentation, upgrade assessments, and knowledge-based articles.
- Leads Microsoft AD related projects independently or through collaboration with team members.

#### **MINIMUM QUALIFICATIONS**

- High school diploma or equivalent.
- 3 years of general experience (relevant accredited coursework may substitute for part).
- 4 years of specialized experience (education may substitute for part).
- 3+ years in Microsoft Entra (Azure) including Identity, Licensing, and Microsoft Purview.
- Strong understanding of identity security best practices, least privilege, and role-based access control.
- Employment contingent on a satisfactory background check (FBI name & fingerprints).
- Advanced experience administering, designing, implementing, and supporting Microsoft Active Directory Domain Services (ADDS) environments, including knowledge of Domain Controllers (DC) configuration and troubleshooting.

#### **BENEFITS**

- Retirement benefits under the Federal Employees Retirement System.
- Optional participation in Federal Employees Health Benefits (FEHB).
- Optional participation in Federal Employees Dental and Vision Insurance Program (FEDVIP).
- Optional participation in Federal Employees' Group Life Insurance (FEGLI).
- Position is excepted service, without competitive civil service tenure.

#### **HOW TO APPLY**

Qualified persons may apply by sending a letter of interest (mentioning announcement 27-02), a résumé, references, and representative writing sample. Experience should be described in detail. Send all required documents in a single PDF document named with applicant's "last name, first name-Announcement 27-02 NITOAD Identity and Access Administrator" by email to [TXW\\_Employment@fd.org](mailto:TXW_Employment@fd.org). 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 reasonable accommodation for any part of the application or interview process, contact Personnel Administrator Michelle Higgins at (210) 981-2081. More than one position may be filled from this announcement. Position announced October 15, 2026, subject to the availability of funds; open until filled. Due to the high volume of applications, only candidates selected for an interview will be contacted.