F. No. 1-5/2003/24(NTISB-II) Islamabad, the 11th October, 2024

Subject: **Cyber Security Advisory – CISA Releases Fresh Active Directory Security Guide (Advisory No. 19)**

Context. CISA has released a guide on detecting and mitigating Active Directory (AD) compromises. AD, central to enterprise IT networks, is a frequent target for cyberattacks due to its complex configuration and legacy protocol support.

2. **Technical Details**. The guide outlines common attack techniques like Kerberoasting, AS-REP Roasting and Password Spraying. It also details mitigation strategies such as implementing Microsoft's Enterprise Access Model, minimizing SPNs, enforcing Kerberos pre-authentication and using Group Managed Service Accounts. Tools like BloodHound and PingCastle are recommended for detecting misconfigurations, enhancing AD security posture against the evolving cyber threats.

3. **Recommendation**. To protect against AD compromises, users and administrators are advised to follow the precautionary measures as well as the specialized tools as suggested by CISA. Also all the AD configurations should undergo a periodic review.

4. Kindly disseminate the above information to all concerned in your organization, attached/affiliated departments and ensure necessary protective measures.