Subject: - **Cyber Security Advisory - Vulnerable IT Infrastructure of Internet Service Providers (ISPs), (Advisory No. 20)**

ISPs provide **internet, email** and **webhosting services** to individuals and organizations. Services of ISPs are either hosted inland or abroad.

2. It has generally been observed that IT infrastructure of ISPs is vulnerable to critical cyber security vulnerabilities. As per analysis, these vulnerabilities include; **SQL Injection, OS Command Injection, Cross Site Scripting, DNS Cache Poisoning, Man in the Middle (MITM)** and **Denial of Service** (DoS) attacks. Exploitation of these vulnerabilities may lead to compromise of ISP's networks. The compromise of network may further result in **data leakage, web defacement** and **hacking of services**.

3. Above in view, PTA is requested to ensure that necessary measures are taken to protect IT infrastructure of ISPs. In this regard, few guidelines are attached at **Appex-I** for onward sharing and further compliance by ISPs.

Appendix-I

VULNERABLE IT INFRASTRUCTURE OF INTERNET SERVICE PROVIDERS (ISPs)

Cyber Security Best Practices for Protection of IT Infrastructure. Few guidelines, but not limited to, are as follows: -

a. **General Security Measures**

(1) Physical security of the facility (ISP/ Server Room) be ensured through **biometric access** to avoid **unauthorized access/ insider threat**.

(2) In case of critical ISPs (providing services to Govt Departments etc), **Security Clearance** of network/ web admin and entire IT Operations team be obtained.

(3) Ensure system updates on regular basis and upgrades be applied as per technological advancements.

(4) **Cyber audit of ISPs** be conducted on **bi-annual basis.**

b. **Technical Measures**

(1) Apply security patches and all software components be updated/ upgraded to latest/ secure versions.

(2) Upgrade SSL servers and services to TLS 1.2 or higher (SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 have known critical vulnerabilities).

(3) All system and network devices are be kept up-to-date.

(4) Cyber Security department be established and standard cyber security policies be defined and implemented.

(5) Admin panels should only be accessible from whitelisted IP addresses.

(6) Vulnerability assessment/ penetration testing/ Cyber Security Audits of all infrastructure and endpoints be carried out on routine basis.

(7) It must be ensured that all data centers and servers are located inland.

(8) Secure transport protocols (such as HTTPS) be used for data in transit.

(9) Applications and databases be installed on different machines, while ensuring system hardening.

(10) Sensitive data be stored in encrypted form with no direct public access.

(11) Security hardening of endpoints and servers be performed and no unnecessary ports and applications be used.

(12) Updated Antivirus tools / Firewalls be used on endpoints and servers to safeguard from potential threats.

(13) Enforce strong password usage polices.

(14) Remote management services like RDP and SSH etc must be disabled in production environment.

(15) Deploy Firewalls for protection against cyberattacks.

(16) Log retention policy must be devised for at least 3x months on separate device.