Subject: - **Cyber Attacks on Pakistan Critical Information Infrastructure and Websites (Advisory No. 22)**

1. Recently, an Indian News Channel was hacked, allegedly by anti-Indian Government elements or non-state actors from Pakistan. Apparently, said hacking incident took place as a reaction to recent blasphemous statements by BJP's leadership. It is anticipated that as a reaction, hostile elements may conduct attacks on Pakistan's Critical Information Infrastructure **(compromise, gain control** or **DDoS attacks)** or vital websites (for **defacement** etc), both in public and private sectors. Possibility of other attack types, by hostile cyber actors for **information gathering, system control, malware distribution, data loss and identity theft** etc, cannot be ruled out. It is, therefore, urged that all concerned be sensitized to adopt **preventive measures** and **proactive monitoring** of systems (attached at **Appendix-I)** to cater for any such incidents.

2. **Pakistan Electronic Media Regulatory Authority (PEMRA) Only.** In wake of above, **PEMRA** to take concrete measures and specifically instruct **Print** and **Electronic Media**, **Government** and **Private** TV channels with its broadcast, **Web** & **YouTube** etc to ensure Cyber Security measures at their end. Separate Guidelines for PEMRA are attached as **Appendix-II**.

2. Disseminate the same message in your organizations, all attached/ affiliated departments and ensure necessary protective measures.

No. [illegible] Chairman's Sectt [illegible] 2022

Appendix-I

Cyber Attacks on Pakistan Critical Information Infrastructure and Websites

1. Few guidelines **(not limited to)** related to preventive and monitoring measures against possible cyber-attacks are as under: -

a. **Preventive Measures**

(1) **For Web Admins**

(a) Defend your website against SQL injection attacks by using input validation technique.

(b) HTTPS protocol be used for communication between client and web server.

(c) Website admin panel should only be accessible via white-listed IPs.

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

(e) Upgrade OS and webserver to latest version.

(f) Employ secure coding practices such as parameterized queries and proper input sanitization and validation to remove malicious scripts.

(2) **For Network & System Admins**

(a) **Network Admins**

(i) Complete analysis and penetration testing of application be carried out to identify potential threats.

(ii) Deploy web application firewalls for protection against web attacks.

(iii) Keep system and network devices up to date.

(iv) Complete website be deployed on inland servers including database and web infrastructure.

(v) Enforce a strong password usage policy.

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

(b) **System admins**

(i) Application and database be installed on different machines with proper security hardening.

(ii) DB users privileges be minimized and limited access be granted inside programming code.

(iii) Proper security hardening of endpoints and servers be performed and no unnecessary ports and applications be used.

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

b. **Monitoring of Services.** To ensure proactive monitoring, organizations/ departments must formulate **Cyber/ Information Security Policies/ SOPs** and implement the same in true letter and spirit. Teams of IT Operations and Security must work in conjunction to ensure smooth provision of services. Few recommended proactive monitoring measures are as under: -

(c) Log retention policy must be devised for at least 3x months on separate device, for attacker's reconnaissance.

(d) Implementation of centralized Log Server/ NMS for central logging and monitoring of network/ systems/ applications.

(e) Conduct of regular cyber/ IS drills to deter preparedness level for emergency situations.

(f) Implementation of **SIEM/ SOC** solution with complete visibility of network and host-based traffic to cater for cyber attacks such as DDoS monitoring etc.

(g) Cyber/ Information Security teams must be formulated to ensure round the clock monitoring from cyber security aspects.

(h) **First party, second party** and **third-party audit** (including **infrastructure, application** and **network**) may be conducted to identify and mitigate possible risk.