Subject: - **Prevention against Website Compromise on the Eve of National Days (Advisory No. 47)**

Context. Hostile elements/ state sponsored malicious actors typically target government departments/ ministries and defence sector websites on the eve of the National Days for disruption of services and defacement to tarnish the global image of Pakistan. It is likely that hostile elements may launch cyberattack on the occasion of Independence Day i.e **14th August, 2023**. Accordingly, an advisory is being sent to sensitize website administrators and Service Providers to take additional security precautions (such as web server hardening, traffic/ integrity monitoring etc) to avoid possible website defacement/ hacking attempts. Moreover, webserver administrators should be made mindful of cyber security guidelines mentioned below.

2. **Cyber Security Best Practices for Websites Protection**

a. **Upgrade OS** and **webservers** to latest version.

b. Website **admin panel** should only be accessible via **white-listed IPs.**

c. Defend your website against SQL injection attacks by using input validation technique.

d. Complete analysis and penetration testing of application be carried out to identify potential threats.

e. Complete website be **deployed on inland servers** including **database** and web infrastructure.

f. **HTTPS** protocol be used for communication between client and web server.

g. **Application** and **database** be installed on **different machines** with proper security **hardening**.

h. Sensitive data be stored in **encrypted** form with **no direct public access**.

i. DB users privileges be minimized and limited access be granted inside programming code.

j. Proper **security hardening of endpoints** and servers be performed and no **unnecessary ports** and applications be used.

k. Updated **Antivirus tools/ Firewalls** be used on both endpoints and servers to safeguard from potential threats.

l. Enforce a strong **password usage policy**.

m. Remote management services like **RDP** and **SSH must be disabled** in production environment.

n. Deploy **web application firewalls** (**WAF**) for protection against web attacks.

o. Employ **secure coding practices** such as parameterized queries, proper input sanitization and validation to remove malicious scripts.

p. Keep **system** and **network devices** up-to-date.

q. **Log retention policy** must be devised for at least 3x months on separate device for attacker's reconnaissance.