GOVERNMENT OF PAKISTAN
CABINET SECRETRIAT, CABINET DIVISION
NATIONAL TELECOM & INFORMATION TECHNOLOGY SECURITY BOARD
(NTISB)

No. 1-5/2003 (NTISB-II) Islamabad 13 Aug 2020

Subject: **Prevention Against Website Compromise (Advisory No. 13)**

1. **Context.** Recently, hostile elements / state actors are actively targeting government / ministries and defense sector websites for disruption and defaming national image of Pakistan internationally. It is likely that hostile elements shall attacks on forth coming national days (14 Aug, 6 Sep). Therefore, it is recommended that system / web administrators of must take extra security precautions like webserver hardening, traffic / integrity monitoring of websites to avoid possible website defacement hacking attempts. Moreover, webserver admins must be made of cyber security guidelines mentioned in attached advisory.

2. **Recommendations**

a. Upgrade OS and webserver 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.

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

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 threat.

l. Enforce a strong password usage policy.

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

M(A)

M(I.T)

Ay.S (Rev. Div.)
18/8

Chief (IT)

Ensure compliance
Obtain certificate
from PRAL

Recommendation - action taken by PRAL - Date of action

Put up as discussed
SS(IT-II)

19/8/2020
Chief (IT)

n. Deploy web application firewalls for protection against web attacks.

o. Employ secure coding practices such as parameterized queries and 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.

3. Forwarded for perusal and dissemination of information to all concerned and under command, please.

Major
(Ch Usman Firdous)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

<u>All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments</u>

Copy to: -

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Special Secretary, Cabinet Division, Islamabad
5. Secretary, NTISB, Cabinet Division, Islamabad
6. Deputy Secretary, NTISB, Cabinet Division, Islamabad
7. Director (IT), Cabinet Division, Islamabad