F. No. 1-5/2005/24(NTISB-II) Islamabad, the 16th February, 2024

28 FEB 2024
C(IT)
C(A&F)

Subject: - **Pakistan's Digital Blackout – Fake Propaganda and Response Initiative at Financial Sector (Advisory No. 03)**

Resilient National Cyber Space and Critical Information Infrastructure (CII) play a significant role in the national security and economy, requiring a comprehensive framework for fail-safe protection. Pakistan's CII is vulnerable to cyber attacks due to non-implementation of requisite cyber security (CS) measures/best practices. Hence, the existing vulnerabilities are not only exploited but also used as an add-on to launch fake propaganda by the Hostile Intelligence Agencies (HIAs).

2. A few examples depicting fake propaganda observed are as under:

M (IR-Ops)
M (IR-P)
M (Cus-Ops)
M (Cus-P)
M (Admn/HR)
M (IT)
M (FATF)
M (Legal)
M (Reforms)
M (Legal & Acc. Cus)
M (Acc. & Audit)
Addl. Secy (Rev. Div.)
SA / SPS

a. **Dec 2023**. An Indian hacker group **"Vanguard"** claimed to have taken down Pakistan's **.gov.pk** domain. Fake propaganda claims disarray of Government agencies, educational institutions and public service websites, leaving the citizens frustrated and businesses scrambling.

b. **Jan 2024**. An Indian hacker group **"UCC Error 404 Team"** claimed to have hacked/defaced Pakistan's critical websites including Govt of Pak, Defence, Aviation and Banking Sector. The fake propaganda made by the hacker group co-related the attack with the Indian Republic Day (26 Jan).

3. Dark Web analysis and the above shared information depicts that threat from a number of hacker groups targeting financial/banking sector of Pakistan is imminent. In the prevailing environment, there is a dire need to ensure implementation of robust CS measures by all Federal Ministries/Divisions, CII especially SBP (in collaboration with Ministry of Finance and Banking sector). It is pertinent to mention that the following advisories on the subject have already been shared with all stakeholders:

a. Cyber Security Advisory - Surge in Financial/Banking Scams & Prevention (Advisory No. 43, dated 4th August, 2023)

b. Cyber Security Advisory - Prevention Against Financial Scam Activities - Impersonation as Govt Officials (Advisory No. 53, dated 8th September, 2023)

FBR eDox Dy.No. 26425R
Received in Chairman's Secti
21 FEB 2024

4. All Ministries/Divisions and SBP are advised to caution affiliated setups and ensure that necessary CS measures/safeguards are in place to deter imminent threat.

5. **SBP Only.** SBP is requested to disseminate the information with the Banking Sector immediately and share certificate of compliance with NTISB (Cabinet Division) on priority.

6. This issues with the approval of the Competent Authority.