Subject: **Protection Against COVID-19 themed Cyber Attacks (Advisory No.6)**

1. **Background.** The National Telecom & Information Technology Security Board (NTISB), working under the aegis of Cabinet Division has been mandated to ensure Telecommunication and Information Technology Security at National Level. To this end all Ministries and Departments are updated by NTISB about emerging threats in the field of Telecom and IT and necessary remedial measure are also suggested by issuing frequent advisories.

2. **Context.** Cyber monitoring reveals that threat actors are actively expl COVID-19 pandemic as and opportunity to lure in their tgts. Attacker spread malicious documents / applications / phishing links as COVID-19 pamphlets to spread information and data stealing Torjans, Malware and Ransomware. Therefore, internet users (especially employees working through teleworking) are advised to be cautious of these attacking techniques and must ensure and follow cyber security best practices.

3. **Summary of COVID-19 Based Cyber Attacks.**

   a. **Spreading Mechanism**. Social Engineering and Email Attachments.

   b. **Reported Email Subjects**.

      (1) COVID-19 Supplies (Masks, Gloves & other products).

      (2) COVID-19 Pandemic map.

      (3) Effects / Symptoms of COVID-19.

      (4) COVID-19 Online Diagnosis.

4. **Indicators of Compromise**

   (1) Blocking / Hacking of social media or email accounts.

   (2) Unexplained financial transactions.

   (3) Identity theft.

   (4) Revealing of organization specific sensitive information publicly

5. **Pakistan Cyberspace**. Since the outbreak of Coronavirus following types of cyber scams have been observed: -

   (1) Malicious Email Attachments.

   (2) Social Engineering Scams.

   (3) Charity Scams.

   (4) Fake Information Links.

   (5) Spending Fake Coronavirus Update Appl.

   (6) Anti Coronavirus Disinfection Teams

6 **Recommendations.**

a. Remain vigilant for **Scams related to Coronavirus Disease 2019 (COVID-19),** as attackers may send emails with malicious attachments or links**to trick victims into revealing sensitive information.**

b. Currently, **no official coronavirus application is available for Windows, Android and iOS.** Therefore, **don't download / install applications sent through SMS / WhatsApp messages.**

c. Utilize 2 factor verification / authentication with Email, Social Media and Banking accounts.

d. Update VPNs, network infrastructure devices and harden endpoints with the latest software patches / security configurations especially those which are being used for remote connections / work from home.

e. **Harden the endpoints used for remote work and block code execution** within enterprise environment to decrease the threat landscape.

f. Install licensed and **update well-reputed anti-virus software.**

g. Don't open **attachments from unknown e-mails.**

h. Enable **personal / domain firewalls on workstation.**

i. **Change default passwords on home WiFi router** to prevent hackers from accessing / exploiting it.

j. Ensure that **remote sessions automatically timeout** after a certain period of inactivity.

k. **Harden web browsers** to block execution of JavaScript and Adobe Flash which is used for most attacks on privacy.

l. **Disable macros permanently in MS Word/PowerPoint / Excel,** as vicitims are actively targeted using macro base malware.

m. For **technical guidance and detailed endpoint protection suggestions / hardening recommendations** contact NTISB on **asntisb2@cabinet.gov.pk**