Subject: **Prevention Against Ransomware Attacks(Advisory No. 3)**

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.** Recently, various Ransomware Malware attacks have surfaced in Pakistan cyberspace. Ransomware encrypts file / folder contents within the system making them inaccessible and demands ransom payment usually in Bitcoins to unlock / decrypt them. Ransomware result in temporary or permanent loss of sensitive information and causes disruption to regular operations and potential harm to an organization's status. Network / System administrators must be familiar with ransomware proliferation mechanisms to prevent or mitigate against such attacks.

3. **Summary of Ransomware Attacks.**

   a. **Spreading Mechanism.** Exploits, Phishing Emails, Software Cracks, RDP.

   b. **Indicators of Compromise.**

      (1) File extensions are changed / encrypted.

      (2) Unable to use / open system files or executable.

      (3) Demands a ransom paymentfor providing the decryptionkey for the encrypted file

   c. **Pakistan Cyber Space.** Some of the **most seen ransomware** in Pakistan's cyberspace are as following: -

      (1) GrandCrab(.crab).

      (2) WannaCry (.wcry).

      (3) Petya / Not Petya.

      (4) Locky Ransomware (.locky).

      (5) Nemuco.

4. **Recommendations.** In this regard, following are recommended: -

   a. Disable **mshta.exe, powershell.exe, cscript.exe, bitsadmin.exe, Regsvr32.exe** and**wscript.exe.**

   b. Don't open **attachments from unknown e-mails,**and forward them to email addressesmentioned in para4.

c. **Implement strict application whitelisting** to block binaries running from **%APPDATA% and %TEMP% paths** as malware generally drops and executes from these locations.
d. Establish a **Sender Policy Framework (SPF), Domain based Message Authentication, Reporting and Conformance (DMARC) and Domains Keys Identified Mail (DKIM) for email domain** to prevent / detection email spoofing through which most of malware samples reaches the email inbox.
e. Perform **regular backups** of critical / sensitive information to help prevent data recovery process.
f. Enable **personal / domain firewalls** on workstation.
g. Disable remote **Desktop Connections** and **restrict RDP using Firewall** to selected remote endpoints preferably using VPN.
h. Don't use **Internet Explorer or Microsoft Edge**as default browsers. Moreover, no unnecessary plug-in must be installed in browsers.
i. Install and update antivirus software on all systems