Subject: **SPECIAL CYBER SECURITY ADVISORY (Advisory No,10) September, 2017**

1. **Introduction.** Threats posed by cyber-attacks are increasing exponentially. Many of networks at national level are vulnerable to cyber-attacks that result in disruption of services and leakage / loss of data. Social media is also being used by hostile elements (foreign and local) to gather sensitive information from officers and staff of the organizations. The same information is used for planning and conduct cyber-attacks against sensitive national networks.

2. **Significant Cyber Attacks on Pakistan**

a. **Operation Hangover — Indian Cyber War.** India is continuously conducting cyber-attacks against officers / staff of government departments with an aim to extract sensitive letters. Recent examples include cyber-attack on some ministries special projects of Pakistan having national / global significance.

b. **Indian Cyber Weapon (Inpage).** India has developed a cyber-weapon specific to Pakistan in the form, of a zero-day exploit of Inpage Software. The software is extensively used in all offices in the country. User who are using free version of Inpage Software can be hacked by India.

c. **WannaCry Ransomware.** WannaCry is a ransomware based cyber-attack which is using a vulnerability present in all windows operating systems called *Etemalblue.* This vulnerability has become public and is being used by hostile agencies / local hackers to hack networks in Pakistan.

3. **Analysis**

a. There is lack of understanding about cyber security at all levels.

b. Lack of requisite cyber security systems, policies and qualified human resource.

c. Due to lack of awareness regarding cyber security, user of organizations get hacked and sensitive letters/data is stolen from their PCs.

d. Due to lack of controls on PCs, Servers and mobiles, rouge insider can leak the data and initiate cyber-attack from within networks.

e. Budget allocation doesn't cater for cyber security.

f. Many organization don't have disaster recovery mechanism.

g. Uncontrolled use of social media, Smart Phones, USB Devices and public email systems are major cause of cyber-attacks in organizations.

4. **Cyber Threat Actors.** Analysis reveal that India is main cyber threat actor against national networks of Pakistan followed by US, Russia, China and many other countries. Even local hackers are conducting cyber-attacks against national networks.

5. **Recommendations**

a. Cyber security be given due importance at all levels.

b. Cyber security policies be implemented in true letter and spirit.

c. Annual budget must cover the funds of cyber security systems and human resource.

d. Vulnerability Assessment and Penetration Testing must be carried out for own servers and applications through reliable local third party companies.

e. Administrators of networks must be well qualified in cyber and information security. They must be security wise cleared.

f. Periodic cyber security trainings be planned at all tiers.

9. Cyber Security hardening of PCs and Servers be carried out to prevent insider threat as well as threat posed by unwary user.

h. Disaster recovery of sensitive data be ensured.

j. Strict controls be ensured to prevent misuse of Social Media, Personal Smart Phones, USB Devices and Public Email Systems.