Subject: - **Advisory - Fresh List of Malicious Appls (Advisory No. 14)**

1. Sequel to already identified 70x malicious apps, **8x new malicious apps (PaighamChat, Skymate, Boss, ChitChat Box, Triover, Hideme, LionVPN & Zepp)** are being used by Hostile Intelligence Agencies (HIAs) for espionage/ information gathering. Newly identified applications are chat-cum-hacking apps developed by Indian Military Intelligence to trap armed forces and civil persons to extract classified information through technical/ coercive (blackmailing) measures.

2. Individuals who have accidently installed any of malicious apps mentioned in **Appendix-I** must immediately perform following actions: -

a. Note down contact details (WhatsApp number/ Facebook ID etc) of suspected individual who shared the link for downloading the application for reporting the same to CSO of own organization/ department.
b. Immediately switch off infected mobile phone (remove battery if possible), remove SIM and disconnect from internet.
c. Share subject information/ incident with all persons/ saved contacts for their security.

3. **Recommendations**. Above in view, following best practices are recommended: -

a. Always check application permissions before installation of application and install applications from Google Play Store only.
b. Under command should regularly be sensitized about malicious actors' tactics, techniques and procedures, moreover, all personnel (officers/ staff) be sensitized to refrain from engaging in activities that may lead to exploitation.
c. Install and update reputed antivirus solution on Android devices like AVAST or Kaspersky. After installation, scan the suspected device with antivirus solutions to detect and clean infections.
d. Before downloading/ installing apps on Android devices, review the app details, number of downloads, user reviews/ comments and "ADDITIONAL INFORMATION" section.
e. In mobile settings, do not enable installation of apps from **"Untrusted Sources"**.
f. Install Android updates and patches as and when available from Android device vendors.

g. Do not download or open attachment in emails received from untrusted sources or unexpectedly received from trusted users and forward them to emails mentioned in para 4.

h. Avoid using insecure and unknown Wi-Fi network as hostile elements use Wi-Fi access points at public places for distributing malicious applications.

i. Use two-factor authentication on all Internet Banking Apps, WhatsApp, social Media and Gmail Accounts.

j. All officers/ staff must be guided to adhere recommended cyber security measures at personal smart appliances.