Subject: - **Cyber Security Advisory – Dubious Adult Chat Applications OV2600T (Advisory No. 02)**

In continuation of Cabinet Division's NTISB letter No. 1-5/2003/24(NTISB-II), dated 25th April, 2022 (Advisory No. 14).

Introduction. Sequel to already identified 104 x malicious apps, 16x new malicious apps are being used by Hostile Intelligence Agencies (HIAs) for espionage/information gathering. Newly identified applications are chat-cum-hacking apps, which are used to trap government officials 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 & 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 government officials.

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.

Appendix I

LIST OF IDENTIFIED MALICIOUS APPLICATIONS

(AS ON 10 JAN 2023)

Ser	Malicious Appl Name	Ser	Malicious Appl Name	Ser	Malicious Appl Name
1.	Rocket Chat	2.	Safe Dialler	3.	Phub
4.	Omegle	5.	U & Me	6.	Babble V3
7.	Privatechat1	8.	Filos	9.	Chat It
10.	Rapid Chat	11.	YoTalk	12.	Porn Hub
13.	Photo Edition	14.	Crypto Chat	15.	TeleChatty
16.	ZoIPER	17.	Babble	18.	Face Call
19.	Buzz	20.	Tweety Chat	21.	VIBES
22.	Converse	23.	Lite It	24.	Hex Chat
25.	Xpress	26.	Chat On	27.	Vmate
28.	Chirrups	29.	Link Up	30.	Safe Chat
31.	Graphic Version	32.	Secure Chat	33.	Lite Chat
34.	Pvt Chat	35.	Guftagu	36.	Cheerio
37.	Free VPN V3	38.	Twin Me	39.	Philions Chat
40.	Just You	41.	CuCu Chat	42.	FM WhatsApp
43.	Quran.Apk	44.	Fruit Chat	45.	Islamic Chat
46.	SecureIt	47.	ZanigV4	48.	Spitfire
49.	FaceChat	50.	Seta / SA News	51.	Wire
52.	FireChat	53.	Cable-1	54.	Privee Chat
55.	Buddy Chat	56.	Stumped	57.	Zong Chat (Beta)
58.	ZangiV2	59.	Media Services	60.	CrazyChat