Subject: - **Cyber Security Advisory - Leakage of Sensitive Data on Dark Web (Advisory No. 53)**

Context. Dark Web is part of WWW and is only accessible using distinctive software to allow users to remain anonymous or untraceable. It provides anonymity, protection from back-tracking and encrypted communication. Dark Web poses novel and formidable challenges to law enforcement agencies around the world.

2. **Dark Web versus Cyber Crimes**. Anonymity offered by Dark Web makes it a gateway to the world of crime and is known as hub of cybercrimes. Dark Web constitutes 96% of total data available on internet.

3. **Dark Web Access Techniques**. Access to dark web is managed by black market administrators. TOR browser (the onion route), I2P (invisible internet project), secure shell tool etc. are commonly used to access dark web. Nonetheless, explicit credentials are still needed to get unrestricted ingress to dark web forums.

4. **Use of Dark Web by Criminals**. Dark/deep web is being used by nefarious mindsets including criminals, terrorists, HIAS and non-state actors. Criminals are constantly inducting latest tools to enhance their attack weaponry. Few primary uses of Dark Web by criminals are as follows: -

a. Digital crimes including hacking, cyber bullying/blackmailing, website defamation, buying zero day exploits/hacking tools, data dumps etc.

b. Access to Personally Identifiable Information (PII) of citizens and key appointments via leaked databases.

c. Scammed financial transactions via leaked banking/personal details.

d. Honey pots to trap civilians and government organizations.

e. Encrypted secure and private communication.

f. Terror financing/money laundering and payments through cryptocurrency.

g. Disseminating extremism, propaganda and publishing news of interest.

h. Radicalization of potential targets.

i. Terrorists' recruitments and trainings.

j. Banned outfits' official statements on websites (anonymity of location).

k. Cross border collaboration and terrorist support.

l. Drug, human, obscene material and weapons trafficking.

m. bounty hunting and ransom attacks.

5. **Recommendations**. Users are advised to put in efforts to protect personal and official data from being exposed to cyber criminals and further leakage on hacking forums/dark web. In this regard, safety guidelines are mentioned in ensuing paras:-

a. **Dark Web Guidelines**

(1) Users are advised to stay away from exploring dark web sources (being unsafe)

(2) Honey pots are already set up by HIAs and cyber criminals to trap civilians and government/intelligence organizations. Users should remain vigilant while surfing we.

(3) Cyber criminals could exploit users/systems leading to hacking and leakage of personal/official data on dark web.

b. **Email/Social Media/Browser/other Apps**

(1) Never forward, click/view link or pictures shared on email/WhatsApp by unknown sources/numbers.

(2) It is mandatory to apply 2x factor authentication on all email, social medial and banking accounts.

(3) One-Time Password (OTP) must never be shared with any one as it can compromise two-factor authentication.

(4) Do not install untrusted software/applications (without digital signature) from third party sources on Windows and Android/iOS phone.

(5) Do not install unnecessary plugins on browsers except Adblock and Adblock plus.

(6) Always install and regularly update reputed antimalware/anti-virus solution on both Windows/Android phones.

c. **Mobile Phone Calls.**

(1) All under command be sensitized not to share personal information, passwords or sensitive information on phone calls.

(2) Vishing calls from unknown numbers must not be trusted and reported to PTA if found suspicious.

(3) To counter social engineering/scam phone call, always ask relevant questions from caller and carefully judge him/her to ensure authenticity.