Subject: - **Cyber Security Advisory – Dark Pink APT (Advisory No. 03)**

Context. Dark Pink (origin unknown) is a new APT group operational since mid-2021 targeting Asian governments and military setups. Recently, analysis of attack on Malaysian Armed Forces (MAF) reveals use of phishing emails and sophisticated attacks on email network by Dark Pink. The APT group uses sophisticated Tactics, Techniques and Procedures (TTPs) that warrants employment of proactive Cyber Security monitoring/mechanism in own government and military setups. In this regard, guidelines are provided in ensuing paras for compliance.

2. **TTPs - Dark Pink APT**. Dark Pink uses techniques such as USB infection and DLL exploitation to exploit systems. Primary means of compromise (unauthorized intrusion and access) is phishing emails.

3. **Guidelines/Preventive Measures**. An APT group may frequently change its techniques, tactics and procedures. Whoever, few preventive measures (but not limited to) are as follows: -

a. **Anti-phishing E-mail Guidelines**

(1) Never open unknown and suspicious emails, link and attachments.

(2) Use email service provider anti-virus scanner before downloading any attachment (trusted ones too)

(3) Timely update all applications and Operating Systems (PC and mobile etc)

(4) Use well reputed and updated anti-virus/anti-malware.

(5) Regularly review applications permission, system running processes and storage utilization

(6) Use separate and complex passwords for each system, mobile, SM accounts, financial and mailing accounts etc.

(7) Never use personal accounts on official systems

(8) Use multi-factor authentication (MFA)/two-factor authentications where possible.

(9) Never share personal details and credentials with unauthorized/suspicious users, websites, applications etc.

(10) Always type URLs in browser rather than clicking on links.

(11) Always open websites with https and avoid visiting http websites.

b. **Anti-Masquerading Guidelines**

(1) **Administrators**

(a) Restrict incoming traffic and user's permissions to maximum extent by implementing system hardening at OS, BIOS and application level.

(b) Unauthorized USB and storage media be blocked via hardening. Also, format USb every time before suing to ensure no malware is propagated from one system to another.

(c) Monitor networks including file hashes, file locations, logins and unsuccessful login attempts.

(d) Use reputed anti-virus, firewalls, IPS/IDS and SIEM solutions.

(e) Use separate servers/routing for offline LAN and online networks.

(f) Allow internet access to specific users on need basis and restrict data usage/ applications rights.

(g) verify software and documents before downloading via digital code-signing technique.

(h) Implement MFA in mailing systems administrator controls and other critical systems.

(i) Always maintain back up of critical data periodically

(j) Regularly change passwords at administrator level

(k) Regularly patch and update all OS, applications and other technical equipment.

c. **Users**

(1) Always re-verify trusted user who has sent email/attachment via secondary means (call, SMS, verbal) before downloading.

(2) Report any suspicious activity to Administrator immediately.

(3) Never keep critical data on online systems and store it in standalone systems.