Subject:- **Advisory - Prevention against Hostile Cyber Espionage (Advisory No. 29)**

1. **Introduction.** Recently, a sharp rise in hostile Cyber espionage operations has been observed. The Hostile Intelligence Agencies (HIAs) are in relentless pursuit to target systems and email accounts of government officials to pilfer sensitive information. It is pertinent to highlight that several **advisories / guidelines** on the subject have already been issued to government department over the period of times, but noncompliance of Cyber Security measures by the government ministries / departments are still being observed which are resulting in leakage of sensitive information. It is again emphasized that **recommendations at Para 2 must be followed in true letter and spirit** to avoid data pilferage.

2. **Recommendations.** Online systems / Laptops have become a necessity for exchange of vital communication, therefore, following best practices must be followed to counter hostile cyber attempts: -

a. Every organization / department should appoint / nominate a trained Cyber Security Officer (CSO) who is responsible for ensuring data / system protection and implementation of Cyber Security best practices.

b. Cyber Security check, compliance and malware focused base level audit of all online / offline systems must be conducted on biannual basis by the CSO.

c. **Online Video Conferences.** In COVID pandemic, office work has become dependent on the use of video conferencing / online collaboration tools such as Zoom, Zoho, Slack and Google Meet etc. Hackers are exploiting this lucrative opportunity to target government departments to extract sensitive data. In this regard, following best practices are recommended: -

1. Do not use online meeting / video conferencing tools for sharing classified information.
2. Use multi-layered and potentially multi-vendor solution as this approach makes it harder for an attacker to penetrate the network.
3. Keep the video conferencing systems and operational systems updated with latest versions of all relevant service packs and security updates.
4. Disable nonessential operating system services / ports.
5. Use a firewall to prevent an unauthorized network traffic.
6. Disable auto-answer to calls in virtual meeting rooms (video conferencing system). Configure call control system to reject unauthorized calls.
7. Enable strong authentication / encryption at audio and video clients.

8. Enable PIN code protection on Virtual Meeting Rooms by using distinct lengthy, unique and randomly generated PIN for each Virtual Meeting Room. Regularly change PIN code of each Virtual Meeting Room.

9. Enable "**Waiting Room**" feature so that host can exercise better control over participants. All participants to join virtual "Waiting Room", after permission by the host.

10. Restrict / disable file transfer, call record feature and limit screen sharing.

d. **System / Network Administrators**

1. All the **IT** systems must be properly hardened at hardware, software and operating system level. Basic hardening guidelines are provided at **Serial 2C(2)** through **Serial 2C(4).**

2. All those Windows commands / utilities not required by the end-users should be blocked for endpoint execution like mshta.exe, bitsadmin.exe, finger.exe, certutil.exe, cipher.exe and syskey.exe.

3. Block execution of scripts with .vbs, .vbe, .hta, .js, .wsh, .wsf, .com, .pif, .ps1 extensions.

4. Blacklist / Block outbound network connections from winword.exe, notepad.exe, explorer.exe, powershell.exe, bitsadmin.exe, mshta.exe, excel.exe and eqnedt32.exe.

5. Centralized Monitoring of endpoint Windows logs must be performed to detect anomalous user behavior.

6. Regularly update antimalware solutions running on endpoints in enterprise environment as well as standalone systems.

7. Educate end-users regarding cyber security best practices and antimalware measures.

8. All email attachments be opened on offline system instead of online systems.

9. Moreover, all attachments sent over email must be password protected and password be shared through an alternative medium.

10. Regularly monitor that aforesaid practices are being followed and conduct surprise checks to ensure that cyber security practices are being followed by the end-users.

e. **Internet Users**

1. Never store official email account’s usernames and passwords in the browsers.
2. Do not open spoofed subject emails and mark these as spam.
3. Never click / login to unknown URLs received in the email.
4. Install reputed and updated antivirus such as Kaspersky that can block known phishing sites.
5. Enable **Two Factor Authentication** on all personal / official email accounts including WhatsApp, Facebook, Instagram and Twitter accounts (especially those linked with social media sites and internet banking).
6. Use reputed browsers like Chrome, Firefox and don not install unnecessary browser plugins / addons except adblock / adblock plus.
7. Do not click on popups and ads displayed during web surfing.

*** * * * ***