Subject: **Advisory – Hacking of Webinar (Advisory No.3)**

1. **Context.** In post COVID pandemic, routine office work has heavily become dependent on the use of video conferencing/ online collaboration tools and chat system. Govt/ private departments are using online video conferencing platforms such as Zoom, Zoho, Slack, Google Meet etc for remote meeting and webinars. Hackers/ state sponsored elements are utilizing this lucrative opportunity to target these platform users to extract sensitive data.

2. **Purpose.** A number of vulnerabilities have been discovered such as remote code execution, credentials stealing, mic and camera access etc in various online video conferencing platforms posing data stealing and privacy threats. Details as under: -

Ser	Platform	Vulnerability
1.	Zoom	• Shares personal information with Facebook • Video conference / calls are vulnerability to eavesdropping • Exposure of windows passwords • Remote code execution to install malicious executable
2.	Skype	• Skype (Android ver) info disclosure vulnerability • Untrusted search path vulnerability in Skype installer (Windows ver) • Stack buffer overflow vulnerability for root access
3.	Google Hangout	Open redirect vulnerability to take complete control of end-user machine
4.	Microsoft Teams	• Squirrel exploit privilege escalation • Cross-site scripting (XSS) vulnerability
5.	Slack	• Allows remote attacker to submit masqueraded link in a slack channel • Session hijacking vulnerability
6.	Zoho	• Cross-site scripting (XSS) vulnerability • Remote code execution to install malicious executable

3. **Cyber Security Concerns / Challenges**

a. Hacking of video conference software accounts due to weak password and security settings.

b. Sensitive Data theft / leakage due to known vulnerabilities / zero-days attacks.

c. Cyber-attacks on operating systems of video conferencing systems.

d. Cyber-attacks on management user interface / APIs of video conferencing servers.

e. DoS / DDoS attacks on video conference servers.

4. **Recommendations.** In this regard, following best practices are suggested: -

a. Do not use online meeting / video conferencing tools for sharing classified information.

b. At sensitive organizations, use multi-layered and potentially multi-vendor solution to avoid same bugs and vulnerabilities across multiple components sharing common code. Multi-layered / multi-vendor approach makes it harder for an attacker to penetrate the network.

c. Keep the video conferencing systems and operational systems updated with latest versions of all relevant service packs and security updates.

d. Disable non-essential operating system services / ports where possible.

e. Use a firewall to prevent unauthorized network traffic from reaching your device. For end-user systems, consider installing a personal firewall.

f. Disable auto-answer to calls in virtual meeting rooms (video conferencing systems). Configure call control system to reject unauthorized calls.

g. Enable strong authentication / encryption at audio and video clients.

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

i. Enable "Waiting Room" feature so that call manager (hosting online meeting) can exercise better control over participants. All participants to join virtual "Waiting Room", after approval by call manager / host.

j. Restrict / disable file transfer, call record feature and limit screen sharing to host.