Video Conferencing

VC cameras, which are not protected with any password or having weak password, could be exploited to eavesdrop into the ongoing video conferencing, monitor calls, read call logs, CDR's of VC, intrude/interrupt ongoing call, etc. The vulnerability could be further exploited through remote maintenance module to switch on the camera and monitor activities. To prevent such attacks:

(i) Set a strong password to manage the VC camera.

(ii) Disable administration interfaces from remote access.

(iii) Disable use of default accounts/passwords.

(iv) Check periodically to detect any misconfigurations or missing patches.

For Secure use of commercial VC solutions for discussions between Governments and parent partner organizations:

(i) A separate system may be designated by the organization. Such system should not store any classified or sensitive information.

(ii) The background for the meeting should be chosen in such a manner (like plain wall, curtains or background option of the VC application) no sensitive documents / surroundings are visible during VC.

(iii) Wherever possible, an isolated Internet connection should be preferred for such VCs. Logical isolation may also be considered for VC systems so that other internal systems are not exposed to the VC network.