

ANNEXURE**I. Mechanism by which the Malicious Software Script impact the ICT infrastructure**

- (i) Exploitation of vulnerabilities in the old versions of Microsoft Windows OS and Microsoft Office products Excel, Word and PPTs used in the ICT system.
- (ii) Network components and network products which are not patched with the latest upgrades with respect to cyber security.
- (iii) Phishing mails.
- (iv) Removable media like Pen drives.
- (v) Lack of update antivirus, firewall, etc.

II. Important and immediate steps need to be taken by the Power Sector companies

- (i) The organizations must audit their ICT network and systems with respect to the upgrades and updates of anti-virus, operating system and other software and apply upgrades and updates immediately.
- (ii) Review security policies for email distribution, screening and usage by all users of power sector companies.
- (iii) Business Network (with email access) and Operational Network should be fully isolated.
- (iv) No use of Word processing software, Power Point, Excel sheets on ICT systems deployed in the operational network.
- (v) All Desktop systems connected on the operational and business network be reviewed with respect to the need for pen drives and other removable media. The pen drives in the operational network should mandatorily be disabled.
- (vi) All Desktop systems/devices to be audited for latest software updates for new version of MS windows. Discontinue use of Window XP or older versions. SMB VI or other similar functions need to be disabled to reduce the cyber incidents.
- (vii) Organization must analyse all outgoing and incoming communication traffic to the operational and business network. Deep Packet Inspection System and Netflow system be installed on appropriate segment of Network for monitoring sensitive application.

- (viii) Analysis of communication traffic to identify suspicious traffic to minimize the impact of already compromised systems or systems with existing backdoors.
- (ix) Sandbox – the use of Microsoft Word, Power Point and Excel to minimize their phishing.
- (x) Organization must disable execution of scripts and Internet cookies.
- (xi) The organization must create white listing of authorized applications for network use and disallow all other applications from using the network.
- (xii) The application white listing will ensure that malware, ransomware etc. are made ineffective in operational and business networks.
- (xiii) No upgrade/update be downloaded and applied directly on the devices connected on the Operational Network. The updates and upgrades be downloaded on separate computer systems, examine its behavior and thereafter applied on the computing devices connected on both Operational and Business Network.