ANNEXURE - II

Suggested some basic remedial measures:

1. Identify the infected computer and disconnect it from LAN/Internet immediately;
2. Hard disks of the infected computer may be formatted after taking backup of data files;
3. Operating systems and applications should be re-installed from clean software;
4. Backup data should be scanned for virus before restoring it;
5. Change passwords of all email and online services from another secure computer;
6. Remove unused or unpatched software from computers, particularly remote desktop software, if any. Also keep all the software, OS, anti-virus/malware software patched and up to date;
7. Check web access firewall for any activities from malicious domains.
8. Block these domains at the firewall;
9. Review privileged accounts and check domain controllers for any new accounts;
10. Periodic password change policy to be implemented along with multi factor authentication where appropriate;
11. Alert security operations team to take extra precautions and educate staff on prevention of phishing attacks;
12. Thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in e-mail;
13. Monitor connection attempts towards the listed blocked/compromised URLs;
14. In addition, any other necessary remedial measure mitigate such threats as felt appropriate by your organization;
15. If any IP address belongs to customer of ISP, the customer may be intimated to take necessary actions as above.