No. T-013 /644-Cyber Security/Coll.1   Dated: 03 April, 2019

To

The Addl SGs: Specialized Zone, Dehra Dun/ Southern Zone, Bangalore/ Northern Zone, Chandigarh/ Western Zone, Jaipur/ Eastern Zone, Kolkata/ Central Zone, Jabalpur/ North-Eastern Zone, Shillong/ Indian Institute of Surveying & Mapping, Hyderabad/ Printing Zone, Dehra Dun.

The Directors: Kerala & Lakshadweep GDC, Thiruvananthapuram/ Karnataka GDC, Bangalore/ Tamilnadu, Puducherry and Andaman & Nicobar Islands GDC, Chennai/ Andhra Pradesh GDC, Hyderabad/ Jammu & Kashmir GDC, Jammu/ Himachal Pradesh GDC, Chandigarh/ Punjab, Haryana & Chandigarh GDC, Chandigarh / Uttarakhand & West Uttar Pradesh GDC, Dehra Dun/ East Uttar Pradesh GDC, Lucknow/ Rajasthan GDC, Jaipur/ Gujarat, Daman & Diu GDC, Gandhinagar/ WB & Sikkim GDC, Kolkata/ Odisha, GDC, Bhubaneswar/ Bihar GDC, Patna/ Jharkhand GDC, Ranchi/ Chhattisgarh GDC, Raipur/ Madhya Pradesh GDC, Jabalpur/ Maharashtra & Goa GDC, Pune/ Assam & Nagaland GDC, Guwahati/ Meghalaya & Arunachal Pradesh GDC, Shillong/ Tripura, Manipur & Mizoram GDC, Silchar/ Survey (Air) & Delhi GDC, New Delhi/ Geodetic & Research Branch, Dehra Dun/ Digital Mapping Centre, Dehra Dun / National GDC, Dehra Dun/ GIS & Remote Sensing Directorate, Hyderabad/ Map Archive & Dissemination Centre, Dehra Dun/ Northern Printing Group, Dehra Dun/ Western Printing Group, Delhi/ Eastern Printing Group, Kolkata/ Southern Printing Group, Hyderabad/ International Boundary Directorate (SGO), New Delhi.

Sub:-   **Cyber Security guidelines – Reg.**

SOI has recently established WAN connectivity across SOI offices for e-office implementation. In view of implementing e-office and ICT in SOI, it is essentially required that adequate sensitization and awareness of cyberspace vulnerability is spread among the officers and staff of your office. It may be brought into the notice of all the concerned that cyberspace is vulnerable to a wide variety of incidents whether intentional or accidental and the data exchanged in cyberspace can be exploited for nefarious purposes. A cyber related incident may be carried out in the form of an organized cyber-attack or an uncontrolled exploit such as computer virus or worms or any malicious software which can cause extensive damage to the information infrastructure or key assets.

It is further informed that regular reports are being generated for SOI VPN which contain intrusion, security intelligence and malware events.

In order to maintain secure cyber environment and to prevent any undesirable cyber related event or incident, following general guidelines are issued for strict compliance:-

1.   Scan computer system regularly with updated antivirus for possible infections and disinfect the same.
2.   Install and maintain updated anti-virus and anti-spyware software at desktop level.
3.   Install and maintain personal desktop firewall.

4. Use only genuine software.
5. Keep up-to-date patches and fixes on the operating system and application software.
6. Exercise caution while opening email attachments.
7. Do not browse un-trusted websites or follow un-trusted links and exercise caution while you click on the link provided in any unsolicited emails.

Pardeep

(Pardeep Singh)
Deputy Director,
for Surveyor General of India

Copy:

1. The DSG (HR)/ DAF/ DSG (Vigil.)/ DSG (Tech.)/ I/c GISTC (SGO) for information and necessary circulation to all sections please.
2. DSG (Adm.) for information and with request to;
   a. Provide complete inventory of the computers and networked devices on SOI WAN.
   b. Provide CISO login credentials for generating CISO reports.

3. I/ c Website.