ENGAGE WITH US

Protection of Critical Information Infrastructure entails a multi-stakeholder approach. NCIIPC engages with Industry, Academia and Independent Cyber Security Professionals in order to address current trends, threats and challenges. NCIIPC supports various avenues for engagement:

Responsible Vulnerability Disclosure Program (RVDP): Share any newly discovered vulnerability related to Critical Information Infrastructure on rvdp@nciipc.gov.in.

Malware Reporting: Malwares may be reported in specified format through NCIIPC website (http://www.nciipc.gov.in/documents/Malware_Report.pdf) or may be shared on mal@nciipc.gov.in.

Incident Reporting: Any cyber security incident related to Critical Information Infrastructure needs to be reported on ir@nciipc.gov.in. The format for the same can be found at http://www.nciipc.gov.in/documents/Incidence_Report.pdf.

Internship Program: NCIIPC offers 4 weeks – 6 months Internship program in the field of cyber security to selected students. Those interested may submit their applications on helpdesk2@nciipc.gov.in.

Research Scholars: Dissertations in Cyber Security related subjects with special reference to Critical Information Infrastructure Protection are encouraged. The detailed proposal for the same may be sent on helpdesk2@nciipc.gov.in.

Training in Niche Technologies: NCIIPC solicits conduct of specialised training in niche technologies under Public Private Partnership. Please refer to SOP on PPP (http://www.nciipc.gov.in/documents/SOP-PPP.pdf).

Cyber Security Solution Providers: Indigenous developers of Cyber Security Solutions to include Hardware, Software, Secure Applications, System Hardening, and Security etc. may send details of their product/proposal on helpdesk2@nciipc.gov.in.

Think Tanks: NCIIPC welcomes any suggestions/initiatives/proposals towards enhancing the cyber security posture of CII from Cyber Security Professionals, Think Tanks, and Regulators who may contact us through helpdesk2@nciipc.gov.in.