Telecom – Cyber Security Incident Response Team (T-CSIRT)

Telecommunication sector is one of the seven critical sectors declared by National Critical Information Infrastructure Protection Centre (NCIIPC) established under the Information Technology Act, 2000.

2. Security of telecommunication sector is one of the most important and critical tasks as health of country's entire digital ecosystem, including all other critical sectors, depend upon robustness and security of telecom sector.

3. Further, it is also important to note that there is a convergence of the data and traditional communication services happening through the technological convergence which assumes significance as all of the social as well as economic sectors of the country rely upon the underlying telecommunications infrastructure.

4. To achieve the objective of secure and robust telecommunication sector, Department of Telecommunications (DoT) has taken various measures including establishment of a Telecom-CSIRT having scope over complete Telecommunication sector of the country.

5. Cyber Security Incident Response Team (CSIRT) is an institutional framework which defines various constituents comprising of experts and supported through orders, instructions, policy guidelines to the stakeholders enabling it to perform, coordinate and support the response to a security incident within a defined constituency.

6. A CSIRT for telecommunication sector of India is designated as Telecom-CSIRT (Telecom-CSIRT).

7. Telecom-CSIRT will function as a two tier structure within its constituency for handling the telecom / cyber incidents in Indian telecom infrastructure. It will work in coordination with CERT-India, other CSIRTs in India and other national or international cyber security stakeholders to tackle cyber incidents in Indian telecom infrastructure, whenever needed.

8. Such functions and coordination includes incident reporting and handling, advice, disseminating knowledge of problems, and working cooperatively to resolve a security incident.

9. Following are the major stakeholders of Telecom-CSIRT:

a) Service providers, i.e. TSPs, ISPs, Long Distance Service Providers (NLD/ILD), GMPCS etc.
b) Department of Telecommunications
c) CERT-India
d) Other CSIRTs and cyber security stakeholders

10. Telecom-CSIRT has been operationalized on 31.01.2023. Head of the T-CSIRT is designated as Director General (Telecom-CSIRT).

11. Telecom-CSIRT will interact with stakeholders, other agencies, organizations using secured / protected communications for sharing of information and coordination for incident responses while maintaining confidentiality, integrity and authenticity on a 24X7 basis.

12. An apex level advisory committee for Telecom-CSIRT has been constituted with the term of reference to make necessary policy and administrative level decisions and provide directions / advice on the activities and operations of the Telecom-CSIRT. An executive committee has also been constituted with the term of reference to monitor the day to day tasks conducted by the Telecom-CSIRT.

13. Following are the core functions of Telecom-CSIRT:

a) Core Functions

i. Incident Reporting – Establish mechanisms for identification of cyber incidents in telecom sector as well as mechanisms for reporting cyber incidents to Telecom-CSIRT.
ii. Incident Response – Operationalize a framework for coordinated incident response with stakeholders.

b) Proactive and Additional Functions

i. Information provision on known vulnerabilities, patches or resolutions of past problems etc. to stakeholders.
ii. Security tools, alerts, advisories to help in incident management.
iii. Technology watch for monitoring new technical developments, emerging threats, attack campaigns, and related trends related to its constituency to help identify future threats and emerging technologies.
iv. Security audits, vulnerability assessments and penetration testing (VAPTs) for strengthening robustness of telecom infrastructure.
v. Awareness and capacity building
vi. Telecom-CSIRT Policies, Procedures, SoPs, Guidelines and FAQs
vii. Post incident activities

14. The maturity of a CSIRT is measured with the Security Incident Management Maturity Model, also called SIM3. The Telecom-CSIRT is under the process of assessment based on SIM3 maturity model.