Government of India
Ministry of Communications
Department of Telecommunications
Telecommunication Engineering Centre
K.L. Bhawan, Janpath, New Delhi-110001
(NGN Division/ एन.जी.एन. प्रभाग)

File No.: 1-1/2025-NGN/TEC/GR-LIM/7 Date: 22.05.2025

Subject: Revision of Standard for Generic Requirement (GR) of "**Monitoring Equipment for Lawful Interception of PSTN/NGN/IMS (TEC 61020:2017)**"

In exercise of the powers conferred by rule 5(2) of the Telecommunications (Framework to Notify Standards, Conformity Assessment and Certification) Rules 2025 The draft Standard for Generic Requirement (GR) of "**Monitoring Equipment for Lawful Interception of PSTN/NGN/IMS (TEC 61020:2017)**" is enclosed herewith for consultation process to enable all stakeholders to provide their comments. The comments may be provided by stakeholders with a soft copy in doc/excel sheet format only, as per the template sheet enclosed herewith as **Annexure-I** through email to director-al.tec-dot@gov.in and ddglte.tec@gov.in at the earliest and latest within sixty days.

Enclosures:

1. Draft Standard No. TEC 61020:2017.
2. Template/Format for providing comments (Annexure-I)

03/06/2025

(Rajvinder Singh)
Director(NGN)TEC
Email director-al.tec-dot@gov.in

To,
All Manufacturers and Stakeholders

Copy to:

1. Sr DDG TEC, for kind information
2. AD(IT), TEC – with request for uploading on TEC website/Portal.
3. AD(IMP&TEP) TEC: with a request for uploading on TBT Enquiry Point

Government of India
Ministry of Communications
Department of Telecommunications
Telecommunication Engineering Centre
K.L. Bhawan, Janpath, New Delhi-110001
(NGN Division/ एन.जी.एन. प्रभाग)

File No.: 1-1/2025-NGN/TEC/GR-LIM Date: 22.05.2025

Subject: Revision of Standard for Generic Requirement (GR) of "**Monitoring Equipment for Lawful Interception of PSTN/NGN/IMS (TEC 61020:2017)**"

The draft Standard for Generic Requirement (GR) of "**Monitoring Equipment for Lawful Interception of PSTN/NGN/IMS (TEC 61020:2017)**" is enclosed herewith for consultation process to enable all stakeholders to provide their comments. The comments may be provided by stakeholders in soft copy in doc/excel sheet as per the template sheet enclosed herewith as **Annexure-I** through email to director-al.tec-dot@gov.in and ddglte.tec@gov.in at the earliest and latest within sixty days.

Enclosures:

1. Draft Standard No. TEC 61020:2017.
2. Template/Format for providing comments (Annexure-I)

22/05/25

(Rajvinder Singh)
Director(NGN)TEC
Email director-al.tec-dot@gov.in

To,
All Manufacturers and Stakeholders

Copy to:

1. Sr DDG TEC, for kind information
2. IMP&TEP Division: for uploading on TBT Enquiry Point

वर्गीय आवश्यकताओं के लिए मानक

टीईसी 61020:2017

(पूर्व सं:टीईसी/जीआर/एसडबल्यू/एलआईएम-001/04/जून-17)

STANDARD FOR GENERIC REQUIREMENTS

TEC 61020:2017

(Earlier No: TEC/GR/SW/LIM-001/04/JUN-17)

पीएसटीएन / एनजीएन / आईएमएस के वैध अवरोधन हेतु निगरानी उपकरण

MONITORING EQUIPMENT FOR LAWFUL INTERCEPTION OF PSTN / NGN / IMS

ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र
खुर्शीदलाल भवन, जनपथ, नई दिल्ली-110001, भारत
TELECOMMUNICATION ENGINEERING CENTRE
KHURSHIDLAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA
www.tec.gov.in

Release 04:   JUN, 2017

Price: Free of Cost

FOREWORD

Telecommunication Engineering Centre (TEC) is the technical arm of Department of Telecommunications (DOT), Government of India. Its activities include:

- Framing of TEC Standards for Generic Requirements for a Product/Equipment, Standards for Interface Requirements for a Product/Equipment, Standards for Service Requirements & Standard document of TEC for Telecom Products and Services
- Formulation of Essential Requirements (ERs) under Mandatory Testing and Certification of Telecom Equipment (MTCTE)
- Field evaluation of Telecom Products and Systems
- Designation of Conformity Assessment Bodies (CABs)/Testing facilities
- Testing & Certification of Telecom products
- Adoption of Standards
- Support to DoT on technical/technology issues

For the purpose of testing, four Regional Telecom Engineering Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

ABSTRACT

This document specifies the Generic Requirements of Monitoring Equipment required to monitor lawfully intercepted of telecommunications in PSTN/ISDN/NGN/IMS networks including international and national long distance by authorized Central & State Government agencies.

CONTENTS

Clause **Particulars** **Page No.**

Chapter 1

Chapter 2

HISTORY SHEET

S.No.	Title	GR No.	Remarks
1.	Lawful Interception and Monitoring	GR/LIM-01/01.OCT2000	Issue 1
2.	Monitoring Equipment for Lawful Interception of PSTN/PLMN	GR/LIM-01/02.MAR2005	Issue 2. Reference to ETSI standard ES 201671
3.	Monitoring Equipment for Lawful Interception of PSTN	TEC/GR/SW/LIM-01/03 .JAN-11	Issue 3
4.	Monitoring Equipment for Lawful Interception of PSTN / NGN / IMS	TEC/GR/SW/LIM-001/04/ JUN-17	Issue 4 (includes NGN/IMS Scenario and in the new format of GR) Note: For IMS (Mobile part), the separate GR of 'TWA' division may be referred.

5.	Monitoring Equipment for Lawful Interception of PSTN / NGN / IMS	TEC 61020:2017 (Earlier No. TEC/GR/SW/LIM-001/04/ JUN-17)	Issue 4 Document number changed as per Revised Numbering scheme of TEC for conversion of existing TEC document to Standard vide document no.4-47/2019-RC/TEC dated 07-09-2020

Note:

1. Since the documents have been renumbered as per revised numbering scheme, kindly refer the Mapping- Listing Table pertaining to old and revised document number available on TEC website www.tec.gov.in/. In case of further clarification, please contact at e mail id adgdoc.tec@gov.in
2. Inside the document, GR may be read as Standard for GR, IR as Standard for IR, SR as Standard for SR and TSTP as TEC Test Guide."

REFERENCES

S.No.	Document No.	Title/Document Name
(I)	: TEC GR/IR/SDs	
1.	TEC/SD/DD/EMC-221/05.OCT-16	Electromagnetic Compatibility Standard for Telecommunication Equipment
2.	SD/CCS-02/03.JAN-2000	National Standard CCS7 for MTP and ISUP
3.	SD/ISN-01/03.OCT-2003	ISDN User Network Interface National Standard
4.	GR/LLT-01/06.APR-2007	Large size Digital Local cum Tandem exchanges
5.	GR/SMS-02/01.JAN-2003	Short Message Service Centre for PSTN/ISDN
6.	TEC/GR/FLA/SMP-001/06/JUN-2010	SMPS Based Power Plants
7.	TEC/GR/TX/BAT-001/04.JUN-2011	Valve Regulated Lead Acid Batteries for high rate of discharge application
(II)	: ITU / ETSI/ IEEE Standard/Recommendations	
1.	ETSI TS 101 671	Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic
2.	ETSI ES 201 671	Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic

3.	ETSI TS 102 235-5	Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia Services
4.	ITU-T G.703	Physical/electrical characteristics of hierarchical digital interfaces
5.	ITU-T G.711	Pulse code modulation (PCM) of voice frequencies
6.	ITU-T Q.554	Transmission characteristics at digital interfaces of digital exchanges
7.	ITU-T Q.811	Lower layer protocol profiles for the Q and X interfaces
8.	3GPP 33.107	Technical Specification Group Services and System Aspects; 3G Security; Lawful Interception Architecture and Functions
9.	3GPP 33.108	Technical Specification Group Services and System Aspects; 3G security; Handover interface for Lawful Interception
10.	ETSI TS 133 107	UMTS, LTE, 3G Security, Lawful Interception architecture & functions (3GPP TS 33.107)
11.	ETSI TS 133 108	UMTS, LTE, 3G Security, Handover interface for LI (3GPP TS 33.108)
(III) : Other Standards		
1.	CISPR 11	Limits and methods of measurement of radio disturbance characteristics of industrial, scientific & medical (ISM) radiofrequency equipment
2.	CISPR 22	Limits and methods of measurement of radio disturbance characteristics of ITE

3.	IEC/EN 61000-4-2	Testing and measurement techniques – Electrostatic discharge immunity test
4.	IEC/EN 61000-4-3	Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test
5.	IEC/EN 61000-4-4	Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test
6.	IEC/EN 61000-4-5	Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test
7.	IEC/EN 61000-4-6	Electromagnetic compatibility (EMC) - Part 4-6: Testing and measurement techniques - Immunity to conducted disturbances, induced by radio-frequency fields
8.	IEC/EN 61000-4-11	Electromagnetic compatibility (EMC) Part 4-11: Testing and measurement techniques Voltage dips, short interruptions and voltage variations immunity tests
9.	IS 13252 / IEC 60950	Information Technology Equipment -- Safety, Part 1: General Requirements

CHAPTER-1

1.0 Introduction

1.1 Interception provides authorized Central & State Governments access to telecommunications and communication related information of a target subscriber of a telecom network. The target administration may be done remotely through electronic interface by authorized agencies of Govt. or by service provider on request from authorized agencies. The interception is done by the telephone exchange which extends the communication content and communication related information to an external monitoring equipment located at the monitoring agency, through LIS equipment.

1.2 The interception and monitoring shall be implemented in such a way that neither the target subscriber nor any other unauthorized person may know about it.

1.3 The interception and monitoring shall not affect the basic and supplementary services of the target.

1.4 (a) For all ITU–T/ETSI/3GPP/IEEE recommendations, TEC standards/specification and other standards referred in this document, the latest release/issue with all associated amendments, addendum and corrigendum shall be applicable.

(b) The RFC documents of IETF are subject to periodic revision. Hence, where ever RFCs are mentioned in this document, the offered product shall meet either the referred RFC or its previous version or its previous draft or its updated version. Wherever a feature of RFC is mentioned, the product shall comply with the part of RFC specifying the feature.

(c) For all IETF RFCs, the interpretation of clauses of RFCs shall be as per RFC 2119

1.5 Functioning or intended use of the equipment shall conform to the prevailing laws/ regulation/instructions of Govt.of India.

1.6 All the requirements described in chapter 2 of this document are suggestive requirements and shall be decided by the purchaser at the time of procurement/ tender as per his requirements. However, the requirements described in Chapter-2 will not be tested/ verified by TEC.

2.0 Description

2.1 This document specifies the Generic Requirements (GR) of Monitoring Equipment required to monitor lawfullyintercepted of telecommunications in PSTN/ISDN/NGN/IMS networks including international and national long distance by authorized Central & State Government agencies. (refer fig 1)

2.2 The system shall interface with LIS/Mediation equipmentover standard defined interfaces.

2.3 **Description of Network Elements/Component**

The general architecture for Lawful Interception and Monitoring System is shown in the figures (fig 1) given below:

2.4 **Definitions:**

2.4.1 **Interception**: Providing access and delivery of a target subscriber's communications and communication related information to authorized Central and State Government agencies.

2.4.2 **Monitoring:** Recording and storing of target subscribers' communications and communication related data by authorized Central and State Government agencies.

2.4.3 **LEA:** Lawful Enforcement Agency of the Government authorised for seeking lawful interception.

2.4.4 **LIS**: Lawful Interception System that is responsible for intercepting, correlating and transparently passing the CC and CRI for a specific target to the LIM at the concerned LEA's end. It includes mediation system and provisioning system as per requirement and distribution of intercepted contents to multiple LIMs/CMS.

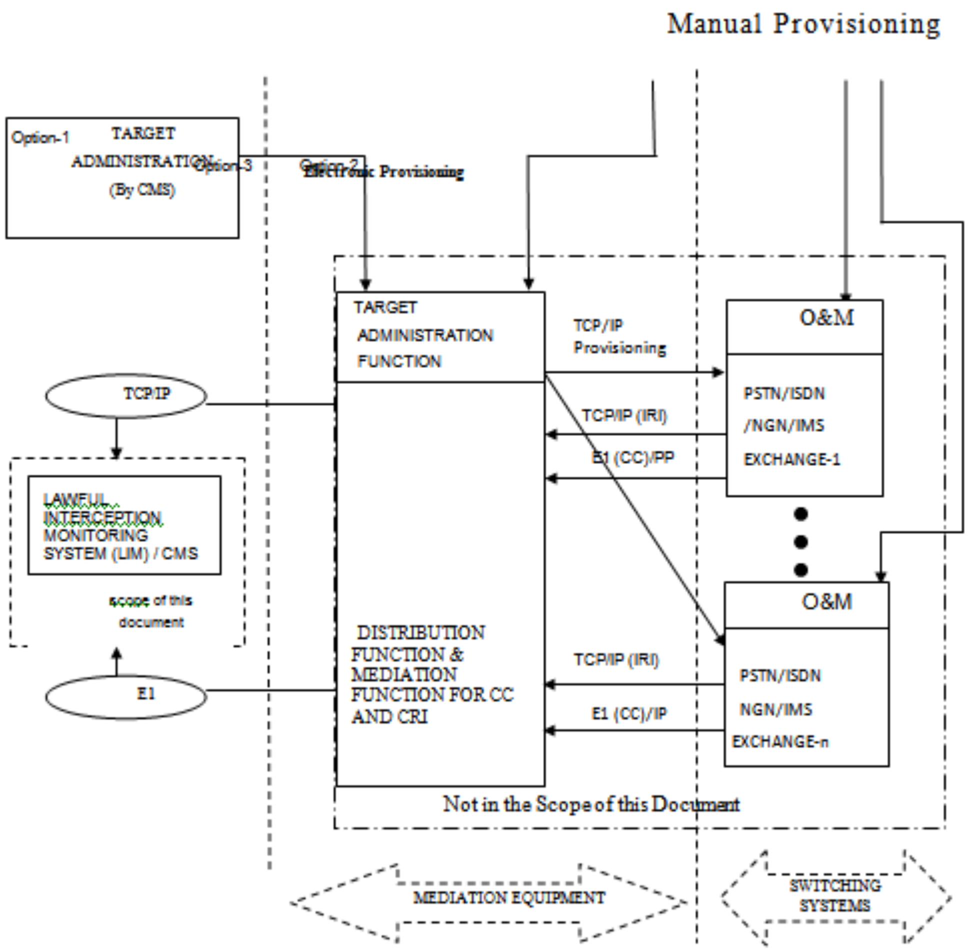
2.4.5 **LIM:** Lawful Interception and Monitoring System available at the LEA's.

2.4.6 **Mediation Equipment**: This is an equipment which passes information between a network operator, an access provider or service provider and a handover interface, and information between the internal network interface and the handover interface. It supplements the Lawful Interception capabilities of a node.

2.4.7 **Target Identity**: Technical identity (e.g. the interception's subjects directory number/IMS identity), which uniquely identifies a target of interception.

2.4.8 **CMS**: Centralized Monitoring System (CMS) is a national level project to centrally monitor the entire country's communication over the TSP & ISP networks for the purpose of lawful interception with end to end electronic Provisioning.

(For Manual Provisioning either Option 1 or Option 2 (not both) should be functional in LIS)


Manual Provisioning
Option-1
TARGET ADMINISTRATION (By CMS)
Option-3
Option-2
Electronic Provisioning
TARGET ADMINISTRATION FUNCTION
TCP/IP Provisioning
O&M
PSTN/ISDN /NGN/IMS EXCHANGE-1
TCP/IP (IRI)
E1 (CC)/PP
TCP/IP
LAWFUL INTERCEPTION MONITORING SYSTEM (LIM) / CMS
scope of this document
E1
DISTRIBUTION FUNCTION & MEDIATION FUNCTION FOR CC AND CRI
TCP/IP (IRI)
E1 (CC)/IP
O&M
PSTN/ISDN NGN/IMS EXCHANGE-n
Not in the Scope of this Document
MEDIATION EQUIPMENT
SWITCHING SYSTEMS

CC- COMMUNICATION CONTENT
IRI- INTERCEPT RELATED INFORMATION
* LIS shall have the capability of both local and remote electronic target provisioning
* Manual Provisioning should either through LIS system or direct. Necessary control can be put as Standard Operating Procedure.

Figure 1: GENERAL ARCHITECTURE FOR LAWFUL INTERCEPTION AND MONITORING

3.0 Functional / Operational Requirements

3.1 General Requirements of Lawful Interception for PSTN Networks

The following requirements of lawful interception system shall be supported by the monitoring equipment (LIM) installed at LEA's end and connected with Fixed line telephony services and/or International Long Distance services.

3.1.1 **Interception Criterion / Targeting Criterion** (Target Assignment):

1. An identity of the subscriber as per E.164 numbering plan/ IMS identity.
2. Part of "Calling Line Number" and "Part of Called Number" as per E.164 Number plan.

3.1.2 Access to Communication Content (CC)

(i) Access to the entire telecommunications transmitted or caused to be transmitted to and from the target subscriber shall be supported for the following forms of telecommunications:

1. Voice,
2. Video,
3. Circuit Switched Data,
4. Fax,
5. Data including SMS from/to Wire line/wireless (Wire line SMS implementation in the network is as per TEC GR No. GR/SMS-02/01.JAN-2003),
6. Any combination of the above forms.

(ii) Signalling messages/ ISUP messages should contain the ETSI correlation parameters namely Lawful Interception Identifier (LIID),Communication Identifier (CID) (which includes CIN & NID) as per the latest version of ETSI TS 101 671, TS 101 232.

It should contain CC Link Identifier (CCLID) parameter in case of Ckt Switching.

3.1.3 Access to Communication Related Information (CRI)

(i) Access to the following data associated with the call/communication shall be supported:

1. Type of call (originating or terminating)
2. Date and time of answer (in case of successful communication)

3. Date and time of call origination (in case of unsuccessful communication)
4. Calling subscriber identity including access code
5. Number dialed by the calling subscriber
6. Indication of bearer capability for ISDN call (speech/ 3.1 kHz / 64 kbps unrestricted)
7. Duration of conversation (Start Time and End Time of the communication)
8. Trunk group & trunk identity (for circuit switching) and relevant equivalent identity in NGN scenario.
9. Cause of termination as per ETSI standard.
10. All the signals emitted by the target subscriber, including post-connection dialed signals, the activation of additional facilities such as conference call, call transfer, call waiting, etc.(including in-band DTMF)
11. Redirecting number (if available)
12. User-to-User information (Content of UUI, Date & of UUI receipt)
13. Lawful Interception Identifier (LIID)
14. Network Identifier (NID)
15. Communication Identity Number (CIN)
16. Communication Identifier (CID)
17. CC Link Identifier (CCLID) for ckt switched calls and equivalent relevant identity for NGN.
18. Missed call alert
    - "Conversation duration" parameter in case of ETSI 101 671 delivery.
    - In case of ETSI 102 232 5 delivery, missed call can be detected by checking call answer indication (call is not answered) and checking release reason of the call (normal, no answer, etc.) in CRI/IRI.

(ii) The communication content and communication related information shall comply with ETSI standards ES 201 671 version 3.1.1 so as to support accurate correlation of communication related information with the communication content. It shall be possible to provide communication related information in both, ETSI and readable format.

(iii) The GUI shall support suitable options so that various fields (as applicable) such as Lawful Interception Identifier (LIID), Communication Identifier CID) (which includes CIN & NID) are configurable as per user requirement.It should contain CC Link Identifier (CCLID) parameter in case of Ckt Switching.In case of CMS, LIID may be used as provisioning parameter.

(iv) All supplementary services reported to Law Enforcement Agency (LEA) by LIS/Mediation equipment as per ETSI standard ES 201 671 version 3.1.1 shall be supported.

(v) **Access to Communication Related Information (CRI) for delivery according to ETSI 102 232 5. (Optional)**

CRI/IRI should include copy of signaling (SIP, H.323, etc.) messages executed on behalf of a target subscriber. Most of CRI information is present in corresponding SIP, H.323 or other signaling messages.

Access to the following data associated with the call/communication shall be supported:

1. Copy of signaling messages. The following are possible options:
   (a) Copy of full IP signaling message including original IP and TCP/UDP headers
   (b) Copy of SIP message content
   (c) Copy of H.323 message content
   (d) Copy of XCAP message content
2. Lawful Interception identifier (LIID)
3. Network Identifier (NID)
4. Communication Identity Number (CIN)
5. Communication Identifier (CID)
6. Time of event

3.1.4 Conditions of Access

(i) Access to a target shall be supported in real time and for full time. Communication content shall be made available at the monitoring centre immediately. Communication related information should be provided immediately. In case of link failure, it should be sent as soon as the link is restored.

(ii) The interception and monitoring shall be implemented in such a way that neither the target subscriber nor any other unauthorized person is aware of it.

(iii) The operation and services (basic & supplementary) of the target subscriber line shall not be affected in any manner.

(iv) Where the target subscriber is a party to a conference call or multi-party call, access to the communication content of all parties to that call and to the communication related information relevant to the target subscriber shall be supported.

(v) It shall be possible to carry out operations required for interception without any interruption to service.

(vi) There shall be no change in the quality of a communication (speech level/data speed /Fax quality/noise online etc.) when it is being monitored and when not being monitored.

(vii) Details of CC and CRI/IRI being monitored by security agencies shall not be available/ accessible to anyone anywhere in the gateway/ switch except to the competent authority, who will be programming the number of interest. Also, details of communications being monitored/ number of interest programmed should not be printed anywhere in the traffic report/ billing information.

3.1.5 Multiple and Simultaneous Monitoring

3.1.5.1 Provision shall exist to monitor a single target subscriber simultaneously by at least TWELVE monitoring agencies.

3.1.5.2 In such cases, each access shall be kept separate and distinct to ensure that the interest of each agency is not known to the others.

3.1.6 Encryption and Encoding

3.1.6.1 The communication content shall be transmitted in its original form without any encryption and encoding, unless otherwise asked for, to the monitoring centre.

3.1.6.2 Where the communication content is modified by the target subscriber, it is the responsibility of the monitoring agency to extract the intelligence from the communication.

3.1.7 **Requirements of the Monitoring Equipment:**

(i) The monitoring equipment shall support recording and storing the communication content and communication related information of at least 480simultaneous calls. The number of activated targets shall be at least 3000.

(ii) The Monitoring Centre shall support the decoding of encrypted call content, if received from the Mediation Equipment and/or Switch. If the switch/NE is encrypting the communication, then the LIS should decrypt the same before delivery.

(iii) Apart from multimedia communication, the monitoring equipment shall also be capable of recognizing the transmission of FAX and data communications and after recognizing, it should store the FAX and data communications target-wise, which should be retrievable and presented in its original form, whenever required. It shall be possible to store FAX as text files.

(iv) Indication for the 'start of the call' (e.g. ring) and 'end of the call' sent by the exchange/LIS shall be detected by the monitoring equipment.

(v) Monitoring equipment shall be capable receiving and storing the communication related information in the system disk for all the communication routed to it.

(vi) Monitoring shall be possible for the entire duration of the communication without losing any part of telecommunications.

(vii) The monitoring equipment shall only receive both way telecommunications between the target and calling/called party. The speech/data from the monitoring equipment/monitoring personnel shall not be mixed with the telecommunications.

(viii) The operation of the target subscriber line shall not be affected in any manner.

(ix) No indication whatsoever should be given to the target subscriber that intercept function has been invoked on the target.

(x) The monitoring shall not affect the basic and supplementary services of the subscribers under monitoring.

(xi) The system shall support the conversion of intercepted data in a readable and audible format and shall support to store the intercepted data on suitable reliable storage media automatically.

(xii) The monitoring centre shall support the following modes of operations:

(a) Target based monitoring: Interception of all telecommunication of target directly from the network.

(b) Online and retroactive analysis of large amount of communication which have been intercepted and stored to locate unknown target and information.

(xiii) The monitoring centre shall support various tools such as 'text search', 'online filtering', 'graphical presentation of communication', 'localization of mobile target' for Interactive analysis.

(xiv) The text search implementation shall be sensitive to misspelling of keywords, grammatical extension of keywords apart from basic string matching capabilities.

(xv) The online filtering shall be activated based on single/multiple call parameters recorded in monitoring centre as Communication Content and Communication Related Information. Filtering shall also be possible based on DTMF generated in call (e.g. for VCC calls) as well as based on partial digits stored in "Calling/Called Number" fields.

(xvi) The monitoring centre shall support both dynamic and static allocation of time slot for the purpose of call content delivery.

3.1.8 System supervision

3.1.8.1 Provision shall be made for continuous testing of the system to allow both system quality check and fault indication as a fault arises.

3.1.8.2 The equipment shall provide for print-outs and visual/audible alarms to assist in efficient administration.

3.1.8.3 The visual display and the devices for manual control of the different parts of the system shall preferably be centralized on a supervisory panel. Details of the displays and the control arrangement shall be provided.

3.1.8.4 In case a fault is detected requiring reloading of the program, this shall be carried out automatically. There shall be a provision for manual-loading of the programs/software modules.

3.1.9 Maintenance facilities

3.1.9.1 The system shall have the capability to monitor its own performance and to detect, analyze, locate, and report faults.

3.1.9.2 The equipment design shall be such that any special care and precautions on the part of the maintenance personnel are kept to an absolute minimum.

3.1.9.3 The maintenance spares supplied shall take into account the MTBF and MTTR. The supplier shall accordingly supply number of spares for a period of 3 years. At least one spare PCB of each type shall be supplied.

3.1.10 Diagnostic capabilities

(i) The diagnostic capability of the system shall be such as to minimize the human efforts required. To this end, the supplier shall indicate how much of the diagnostic program are normally resident in the on line program. Details of the off-line diagnostic program shall be given. The procedure for invoking such program shall be described. The procedure for consulting fault dictionary for diagnostic program shall be made available.

(ii) All the hardware testers necessary for efficient maintenance of the system shall be provided. Details of the testers shall be indicated.

(iii) The test procedures, recommended for efficient maintenance of the system, shall be indicated. This shall include details of the testes, their periodicity, etc.

(iv) Any malfunction in the system shall initiate a fault message and/or visible and audible alarm. The fault information shall direct personal to the appropriate maintenance manual for location of the fault unit or for detailed procedures on further action to be taken for rectification of the fault conditions. The classification of alarms in the system shall be indicated.

(v) A suitable alarm and display system shall be provided for a continuous indication of the system status. Provision shall be available to extend the alarm indication to centralized place.

3.1.11 Storage

(i) Adequate capacity for the purpose of storage and playing back for the various forms of communication content i.e. voice, fax and data shall be provided. The supplier shall provide details for the calculation of disk capacity.

(ii) The communication content for each target shall be stored in a separate area in the disk. It shall be possible to retrieve and present the communication contents, target-wise to an operator at a monitoring position, whenever requested through man-machine commands/GUI.

(iii) The equipment shall be capable of storing at least 2000 hoursof uncompressed signals in the duplicate system disk. It shall be possible to transfer the contents of the storage to a magnetic media e.g. audio tapes, optical discs etc.

3.1.12 Monitoring Positions

(i) It shall be possible to present the communication content in real-time to an operator at monitoring position for a target specified through man-machine commands.

(ii) The communication content for each target shall be stored in a separate area. It shall be possible to retrieve and present the communication contents, target-wise and date-wise to an operator at a monitoring position, whenever requested through man-machine commands.

(iii) Adequate number of monitoring positions with associated hardware and software shall be supported as per the user requirements.

3.1.13 Power Supply: -

i. The equipment shall be capable of working with an input AC Mains supply of 230 Volts with a tolerance of -15% to 10 % and frequency of 50 Hz ± 2 Hz. Or DC power supply of -48V (varies from - 40V to -57V).

ii. Switching mode Power Supply (SMPS) and VRLA battery to be used shall be as per TEC Generic Requirements No. TEC/GR/FLA/SMP-001/06/JUN-2010 and TEC/GR/TX/BAT-001/04.JUN-2011 respectively. Power supply and battery shall be modular and expandable to support the ultimate equipment configuration.

iii. UPS and other power requirements are to be specified by the system supplier.

3.1.14 HARDWARE REQUIREMENTS

(i) Compact and high-performance state-of-the-art hardware shall be used.

(ii) The hardware platform shall be open-ended and modular in architecture so that the equipment can be augmented and adapted to customer requirements.

(iii) The system shall have adequate redundancy so that the total system availability is 99.999% or better for the duration of the monitoring and the communication content and communication related information shall be stored in full without losing any part of the communications.

(iv) Adequate redundancy shall be built into the design of the system so that failure of a single sub-system does not affect the performance and the features of the monitoring equipment.

(v) The system shall be comprised of different units for processing sub-system, network Interfaces, Storage, monitoring positions and User interfaces for operation and management.

(vi) Processing sub-system: The equipment shall have a redundant processor configuration working in active and hot standby mode. Each processor shall have its own hard-disk for main storage. The data in the stand-by disk should be updated periodically from the active disk. In case of failure of the active processor, the standby processor shall become active automatically with zero downtime.

3.1.15 SOFTWARE REQUIREMENTS

(i) The software shall be open-ended and modular in architecture so that the entire system can be augmented and adapted to customer requirements. It shall be possible for LEA to load and integrate software for advance features related to language, speech and accent identifications.

(ii) The normal operation shall not be affected while undertaking software updates, enhancement of features or correction to programs.

(iii) The software shall conform to the following characteristics:

(a) The design of the software shall be such that the system is easy to handle both during installation and normal operations.

(b) The functional modularity of the software shall permit introduction of changes wherever necessary with least impact on other modules.

(c) Adequate flexibility shall be available to easily adopt changes in technological evolution in hardware.

(d) The software shall provide sufficient checks to monitor the correct functioning of the system.

(e) Test programs shall include fault tracing for detection and localization of system faults.

(f) Facilities shall be in-built to ensure automatic system reconfiguration on detection of any major software fault.

(iv) The system hardware/software shall not pose any problem due to change in date and time by events such as changeover of leap year etc., in normal functioning of the system.

3.1.16 Purging

The system should provide automatic and manual purging facility to take care of data deletion as per The Indian Telegraph Rule 419 (A) and The Indian Telegraph Act, 1885 para 5 (2).

4.0 Interface Requirements

4.1 Interfaces between mediation equipment and monitoring equipment:

4.1.1 Interface for transmission of communication content

(i) The system shall be capable of terminating at least ten numbers of 30 Channel PCM links at 2048 kbps as per ITU-T G.703 for receiving the communication content of the target (Voice, FAX, data) coming from the LIS/Mediation equipment. Voice will be received according to ITU-T G.711, A-law encoding. (content delivery as per ETSI TS 133107 &133108 in IMS scenario and as per ETSI 101 671 / 102 232-5 standard in PSTN/NGN scenario)

(ii) Signalling: The Signalling between the mediation equipment and the monitoring equipment shall be one of the following:

- CCS7 as per National standards for MTP and ISUP No. SD/CCS-02/03.JAN-2000.
- ISDN PRI as per TEC SD No. SD/ISN-01/03.OCT-2003.
- IP delivery as per latest ETSI TS 102 232 5
- IP delivery of IMS data as per ETSI TS 133 107 & 133 108.

(iii) The delivery of the communication content to the LEMF with appropriate security measures shall conform to the standard Hand over interface 3(HI3) as per ETSI standard ES 201 671 V3.1.1.

(iv) The security measures such as Access verification, Access protection and Authentication while delivering the communication content shall be as per following ETSI Standards.

- ETSI TS 101 671 V3.14.1 (2016-03)
- ETSI TS 102 232-5 V3.7.1 (2017-03)
- ETSI TS 133 107 V14.1.0 (2017-04) – ETSI version of 3GPP TS 33.107
- ETSI TS 133 108 V14.0.0 (2017-04) – ETSI version of 3GPP TS 33.108

4.1.2 Interface for Transmission of Communication related information:

(i) The interface between the mediation equipment and the equipment at the monitoring agency for transmission of communication related information to monitoring agency in real-time shall beTCP/IP protocol using FTP/SFTPfor data transfer.

(ii) The data transfer protocolfor receiving the call related information between monitoring equipment and mediation equipment shall be compatible.

(iii) It shall be possible to accurately correlate the communication related information with the corresponding communication content. The delivery of this information shall conform to the Hand over interface 2 (HI2) as per ETSI ES 201 671 V 3.1.1.

4.1.3 **Interface between the mediation equipment and the equipment at the monitoring agency**: (For both CC & CRI/IRI)

Interface should be capable to receive the combined Communication Content (CC) & Communication related according to ETSI 102 232 5 standard.

4.2 **Timing:**

1. If all the PCM links terminated on the equipment come from one exchange, then the equipment shall be capable of recovering the clock from one of the PCM links for timing purposes.
2. If PCM links from different exchanges are terminated on the monitoring equipment, the equipment shall be capable of synchronizing to an incoming timing reference. The equipment shall be capable of synchronizing with 2048 kHz analog clock.
3. The minimum hold-over stability of the local clock in the monitoring equipment shall be at least 1 x 10^{-9} per day.

4.3 **Slip:** Under synchronized condition, slip observed on the PCM links shall be less than or equal to 2 slips in 24 hours.

4.4 **Selection of priority:** Equipment shall be capable of selecting the input timing reference depending on the pre-set priority.

4.5 **Jitter Tolerance**

The equipment shall be able to tolerate the following jitter in the incoming 2048 kbps PCM coming from the exchange without losing synchronization:

Frequency	Jitter Amp to be applied Peak to Peak (UI) **	Status of Exchange clock
20 Hz	1.5	Synch mode
2.4 KHz	1.5	--do--
18 KHz	0.2	--do--
100 KHz	0.2	--do--

** For 2048 Kbps 1 UI = 488 ns.

4.6 **Traffic statistics:Traffic report shall** be generated by the equipment for each PCM link separately.

4.7 **Transmission parameters**

Transmission characteristics at 2048 kbps digital interfaces as per ITU-T Recommendation Q.554 are applicable.

BER: BER shall be better than 1 in 10^9 for a 64 kbps connection.

4.8 **Group delay: Group delay shall meet the following requirements:**

Frequency	Permitted limit
(Hz)	*(micro seconds)*
500	900
604	900
1000	900
1792	900
2604	900
2792	900

Note: 900 micro seconds is the mean value. However, the limit for 0.95 probability of not exceeding is 1500 micro seconds.

5.0 Quality Requirements

5.1 Qualitative Requirements (QR):

5.1.1 The supplier/manufacturer shall conform to ISO 9001:2008 certifications. A quality plan describing the quality assurance system followed the manufacturer shall be required to be submitted.

5.1.2 The equipment shall confirm to the requirements for Environment specified in QM 333{issue march 2010}:” Standards for Environmental Testing of Telecommunication Equipment” for operation, transportation and storage.

5.1.3 The failure of any component/subsystem in the system shall not result in the failure of complete system.

5.1.4 List of all components for which second source is not available should be provided.

5.2 Reliability and quality of service:

For the duration of the interception, the reliability of services supporting the interception shall be at least equal to the reliability of the services provided to the target. The quality of service of the intercepted transmissions forwarded to the monitoring facility shall comply to the performance standards of the network operator.

6.0 EMI/EMC Requirements

6.1 The equipment shall conform to the following EMC requirements for Class A:

General Electromagnetic Compatibility (EMC) Requirements: - The equipment shall conform to the EMC requirements as per the following standards and limits indicated therein. A test certificate and test report shall be furnished from an accredited test agency.

a) Conducted and radiated emission(applicable to telecom equipment):

Name of EMC Standard: "CISPR 22 (2008) - Limits and methods of measurement of radio disturbance characteristics of Information Technology Equipment".

Limits: -

i. To comply with Class B **OR** Class A of CISPR 22 (2008).

ii. The values of limits shall be as per TEC Standard No. **TEC/SD/DD/EMC-221/05.OCT-16.**

iii. For Radiated Emission tests, limits below 1 GHz shall be as per Table 4 (a) or 5 (a) for measuring distance of 10m **OR** Table 4 (a1) or 5 (a1) for measuring distance of 3m.

OR

Conducted and radiated emission (applicable to instruments such as power meter, frequency counter etc.):

Name of EMC Standard: "CISPR 11 {2015}- Industrial, scientific and medical

(ISM) radio- frequency Equipment-Electromagnetic disturbance characteristics-

Limits and methods of measurement"

Limits: -

i. To comply with the category of Group 1 of Class A of CISPR 11 {2015}

ii. The values of limits shall be as per clause No. 8.5.2 of TEC Standard No.**TEC/SD/DD/EMC-221/05.OCT-16**.

b) **Immunity to Electrostatic discharge:**

Name of EMC Standard: IEC 61000-4-2 {2008) "Testing and measurement techniques of Electrostatic discharge immunity test".

Limits: -

i. Contact discharge level 2 {± 4 kV} or higher voltage;
ii. Air discharge level 3 {± 8 kV} or higher voltage;

c) **Immunity to radiated RF**:

Name of EMC Standard: IEC 61000-4-3 (2010) "Testing and measurement techniques-Radiated RF Electromagnetic Field Immunity test"

Limits:-

For Telecom Equipment and Telecom Terminal Equipment with Voice interface (s)

i. Under Test level 2 {Test field strength of 3 V/m} for general purposes in frequency range 80 MHz to 1000 MHz and
ii. Under test level 3 (10 V/m) for protection against digital radio telephones and other RF devices in frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz.

For Telecom Terminal Equipment without Voice interface (s)

Under Test level 2 {Test field strength of 3 V/m} for general purposes in frequency range 80 MHz to 1000 MHz and for protection against digital radio telephones and other RF devices in frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz.

d) **Immunity to fast transients (burst):**

Name of EMC Standard:IEC 61000- 4- 4 {2012) "Testing and measurement techniques of electrical fast transients/burst immunity test"

Limits:-

Test Level 2 i.e. a) 1 kV for AC/DC power lines; b) 0. 5 kV for signal /

control / data / telecom lines;

e) Immunity to surges:

Name of EMC Standard: IEC 61000-4-5 (2014) “Testing & Measurement techniques for Surge immunity test"

Limits:-

i. For mains power input ports: (a)2 kV peak open circuit voltage for line to ground coupling (b) 1 kV peak open circuit voltage for line to line coupling

ii. For telecom ports: (a) 2 kV peak open circuit voltage for line to ground (b)2 kV peak open circuit voltage for line to line coupling.

f) Immunity to conducted disturbance induced by Radio frequency fields:

Name of EMC Standard: IEC 61000-4-6 (2013) "Testing & measurement Techniques-Immunity to conducted disturbances induced by radio-frequency fields”

Limits:-

Under the test level 2 {3 V r.m.s.}in the frequency range 150 kHz-80 MHz for AC / DC lines and Signal /Control/telecom lines.

g) Immunity to voltage dips & short interruptions (applicable to only ac mains power input ports, if any):

Name of EMC Standard: IEC 61000-4-11 (2004) “Testing & measurement techniques- voltage dips, short interruptions and voltage variations immunity tests”

Limits:-

i. a voltage dip corresponding to a reduction of the supply voltage of 30% for 500ms (i.e. 70 % supply voltage for 500ms)

ii. a voltage dip corresponding to a reduction of the supply voltage of 60% for 200ms; (i.e. 40% supply voltage for 200ms)

iii. a voltage interruption corresponding to a reduction of supply voltage of > 95% for 5s.

iv. a voltage interruption corresponding to a reduction of supply voltage of >95% for 10ms.

Note 1: Classification of the equipment:

Class B: Class B is a category of apparatus which satisfies the class B disturbance
limits. Class B is intended primarily for use in the domestic environment and may include:

- Equipment with no fixed place of use; for example, portable equipment powered by built in batteries;
- Telecommunication terminal equipment powered by the telecommunication networks
- Personal computers and auxiliary connected equipment.

Please note that the domestic environment is an environment where the use of broadcast radio and television receivers may be expected within a distance of 10 m of the apparatus connected.

Class A: Class A is a category of all other equipment, which satisfies the class A limits but not the class B limits.

Note 2: The test agency for EMC tests shall be an accredited agency and details ofaccreditation shall be submitted.

Note 3: For checking compliance with the above EMC requirements, the method of measurements shall be in accordance with TEC Standard No. **TEC/SD/DD/EMC-221/05.OCT-16**and the references mentioned therein unless otherwise specified specifically. Alternatively, corresponding relevant Euro Norms of the above IEC/CISPR standards are also acceptable subject to the condition that frequency range and test level are met as per above mentioned sub clauses (a) to (g) and TEC Standard No.**TEC/SD/DD/EMC-**

221/05.OCT-16. The details of IEC/CISPR and their corresponding Euro Norms are as follows:

IEC/CISPR	**Euro Norm**
CISPR 11	EN 55011
CISPR 22	EN 55022
IEC 61000-4-2	EN 61000-4-2
IEC 61000-4-3	EN 61000-4-3
IEC 61000-4-4	EN 61000-4-4
IEC 61000-4-5	EN 61000-4-5
IEC 61000-4-6	EN 61000-4-6
IEC 61000-4-11	EN 61000-4-11

The manufacturer / supplier shall submit a test certificate and test report for EMI/EMC compliance from test agency. The test agency for EMI/EMC tests shall be an accredited agency and details of accreditation shall be submitted.

7.0 Safety Requirements

7.1 The equipment shall conform to IS 13252 part 1:2010- “Information Technology Equipment – Safety- Part 1: General Requirements” [equivalent to IEC 60950-1 {2005} “Information Technology Equipment – Safety- Part 1: General Requirements” and

7.2 A test certificate and test report shall be furnished from an accredited test agency.

7.3 The test agency for safety requirements tests shall be an ISO 17025 accredited agency and details of accreditation shall be submitted.

8.0 Security Requirements

8.1 Security aspects

8.1.1 Secure data network arrangements shall be provided between monitoring centre and the exchange for the intercept function commands.

8.1.2 Provision of periodic target synchronization shall be available between monitoring centre and the exchange to ensure that targets already defined have not been removed and unapproved targets have not been included in defined targets in the exchange, when target administration is done by LEA.

8.1.3 The authorized user of the LEA shall be able to start the target synchronization process manually, whenever necessary.

8.1.4 Secure network arrangements shall be provided between Network Element and the monitoring agency to ensure that network related data and the communication content reaches only the appropriate authorities.

8.1.5 Suitable safeguards shall be provided in the man-machine communication program to debar unauthorized persons from making any changes in the memory contents or office data. Access to system operations shall be controlled through multi-level password and authentication check.

8.1.6 It shall be possible to create multiple and separate password authorizations for different functions such as system administrator, security administrator, target administrator etc. according to the needs of LEA by GUI.

8.1.7 Suitable safeguards for security of Mediation Equipment like protection from public domain, safe retention of information/data/observation shall be there.

8.1.8 It shall not be possible for non-authorized personnel to get access to the monitoring equipment, communication content, communication related information and the list of target subscribers.

8.1.9 The system shall support secure reception of data on IP interface using IP-SEC.

8.1.10 The system shall support encryption between mediation equipment and monitoring centre.

8.1.11 The system shall have provision for protection against viruses, worms and other vulnerabilities / threats with regular updates.

8.1.12 No indication whatsoever should be given to any O&M personnel or the target subscriber that intercepts function has been invoked on the target.

9.0 OTHER MANDATORY REQUIREMENTS

9.1 Man-Machine Commands

The operation and management features specified below are in addition to those specified in TEC GR No.GR/LLT-01/06.APR-2007.

9.1.1 The operations related to line interception and monitoring shall be supported by the following (minimum set) of MML commands:

1. Add: To create a target on request from an authorized monitoring agency.
2. Remove: To remove a target from interception on request from an authorized monitoring agency.
3. List: Interrogation of one or all the targets with print-out of all details.

9.1.2 It shall be possible to retrieve the communication related information stored in the exchange selected on the following criteria:

(i) Date
(ii) Target
(iii) Calling number
(iv) Called number
(v) Time

9.1.3 Access to all MML commands related to line interception and monitoring shall be controlled through a multi-level password mechanism.

9.1.4 It shall be possible to store all the commands and responses related to interception given from the O&M terminals in the exchange, in a 'command log' in the system disk, which is separate from the normal 'command log'. This command log shall be a 'read only' file, which can be read by authorized personnel whenever required, using MML.

9.1.5 Hand over interface for target administration shall be supported, if required by the service provider.

9.1.6 The MML shall support suitable commands so that various fields (as applicable) such as Lawful Interception Identifier (LIID), Communication Identifier CID) (which includes CIN & NID) are configurable as per user requirement. It should contain CC Link Identifier (CCLID) parameter in case of Ckt Switching. In case of CMS, LIID may be used as provisioning parameter.

CHAPTER-2

10.0 Information for the procurer of product

1. Typical Data Storage capacity in terms of usable disk space may be 4.5 TB.
2. Sever should be rack mountable.
3. Rack should have biometric control to provide secure access.
4. Should support additional number of drive bays for future expansion of usable disk space.
5. Should have proper back-up mechanism using Tape Drive.

ABBREVIATIONS

3GPP	3rd Generation Partnership Project
ADMF	Administrative Function
BRI	Basic Rate Interface
CC	Communication Content
CCLID	CC Link Identifier
CCS7	Common Channel Signalling No. 7
CD	Compact Disk
CIN	Communication Identity Number
CID	Communication Identifier
CMS	Centralized Monitoring System
CRI	Communication Related Information
DID	Direct Inward Dialing
DTMF	Dual Tone Multi-frequency Signaling
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
GR	Generic Requirement
GUI	Graphic User Interface
IEEE	Institute of Electrical and Electronics Engineers
IMS	IP Multimedia Subsystem
IP	Internet Protocol

IRI	Interception Related Information
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ISUP	ISDN User Part
ITU	International Telecommunication Union
LEA	Law Enforcement Agency
LIID	Lawful Interception Identifier
LEMF	Law Enforcement Monitoring Facility
LIM	Lawful Interception Monitoring
LIS	Lawful Interception System
MMC	Man Machine Commands
MML	Man Machine Language
MTP	Message Transfer Part
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
NGN	Next Generation Network
NID	Network Identifier
PABX	Private Automatic Branch Exchange
PCM	Pulse Code Modulation
PRI	Primary rate Interface
PSTN	Public Switched Telephone Network
RFC	Request For Comment
SFTP	SSH File Transfer Protocol

SIP	Session Initiation Protocol
SMPS	Switch Mode Power Supply
SMS	Short Message Service
TCP	Transmission Control Protocol
TSP	Telecom Service Provider
TWA	Terrestrial Wireless Access
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Universal Resource Locater
UUI	User-to-User Information
VRLA	Valve Regulated Lead Acid
XCAP	XML Configuration Access Protocol

======== End of the document ========

Annexure I

<u>Comments on draft standards for Generic Requirements(GR) of Monitoring Equipment for lawful interception of PSTN / NGN / IMS</u>

Name:

Organisation:

Contact Details:

S.No	Clause No	Clause	Comments	Other Remarks(if any)