Template for submitting comments/inputs on draft Test Guide titled "MONITORING EQUIPMENT FOR LAWFUL INTERCEPTION OF PSTN / NGN / IMS"

(Draft Test Guide No. TEC/TG/SW/LIM-301/01/SEP-17)

Name of Manufacturer/Stakeholder:

Organisation:

Contact Details:

S. No	Clause No.	Clause	Comments	Other Remarks, if any

Note: The comments/inputs on the draft Test Guide (Draft Test Guide No. **TEC/TG/SW/LIM-301/01/SEP-17**) may be provided in the above format vide email to **director-al.tec-dot@gov.in, ddglte.tec@gov.in**

अनंतिम परीक्षण अनुसूची और परीक्षण प्रक्रिया

सं: टीईसी/टीजी/एसडबल्यू/एलआईएम-301/01/सितंबर-17

PROVISIONAL TEST SCHEDULE & TEST PROCEDURE

No. : TEC/TG/SW/LIM-301/01/SEP-17

पीएसटीएन / एनजीएन / आईएमएस के वैध अवरोधन हेतु निगरानी उपकरण

MONITORING EQUIPMENT FOR LAWFUL INTERCEPTION OF PSTN / NGN / IMS

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

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

दूर

संचार अभियांत्रिकी केंद्र

खुर्शीदलाल भवन, जनपथ, नई दिल्ली-110001, भारत

TELECOMMUNICATION ENGINEERING CENTRE

KHURSHIDLAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA

www.tec.gov.in

CONTENTS

A. INTRODUCTION

This document enumerates detailed test schedule and procedure for evaluating conformance / functionality / requirements / performance of "MONITORING EQUIPMENT FOR LAWFUL INTERCEPTION OF PSTN / NGN / IMS" as per GR No TEC/GR/SW/LIM-001/04/JUN-17.

B. HISTORY SHEET

Sl. No.	TSTP No.	Equipment/Interface	Issue
1.	TEC/TG/SW/LIM-301/01/SEP-17	MONITORING EQUIPMENT FOR LAWFUL INTERCEPTION OF PSTN / NGN / IMS	01

C. General information:

Sn.	General Information	Details *(to be filled by testing team)*	
1	Name and Address of the Applicant		
2	Date of Registration		
3	Name and No. of GR/IR/Applicant's Spec. against which the approval sought		
4	Details of Equipment		
	Type of Equipment	Model No.	Serial No.
(i)			
(ii)			
5	Any other relevant Information:-		

D. Testing team: *(to be filled by testing team)*

Sno.	Name	Designation	Organization	Signature
1.				
2.				

E. List of the Test Instruments:

Sno.	Name of the test instrument	Make /Model *(to be filled by testing team)*	Validity of calibration *(to be filled by testing team)*
1			dd/mm/yyy
2			
3			
4			
5			
6			
7			
8			

F. Equipment Configuration Offered: *(to be filled by testing team)*

(a) <Equipment/product name> Configuration:

S.No.	Item	Details	Remarks

Relevant information like No. of cards, ports, slots, interfaces, size etc. may be filled as applicable for the product

(b) <Other equipment name> Configuration:

S.No.	Item	Details	Remarks

Relevant information like No. of cards, ports, slots, interfaces, size etc. may be filled as applicable for the product

G. Equipment/System Manuals: *(to be filled by testing team)*

Availability of Maintenance manuals, Installation manual, Repair manual & User Manual etc. **(Y/N)**

H. Clause-wise Test Type and Test No.:

Clause No.	*Clause*	*Type of Test / Test No. etc. **	*No. of Hours required in testing (approximate/tentative)*
1.0	**Introduction**	Heading	-
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.	Information	-
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.	Information	-
1.3	The interception and monitoring shall not affect the basic and supplementary services of the target.	Information	-
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.	Information	-
1.5	Functioning or intended use of the equipment shall conform to the prevailing laws/ regulation/instructions of Govt. of India.	Undertaking from the Applicant	-
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.	Information	-
2.0	**Description**	Heading	-
2.1	This document specifies the Generic Requirements (GR) of switching systems and Mediation equipment for lawful interception of telecommunications in PSTN/ISDN/NGN/IMS networks including international and national long distance by authorized Central & State Government agencies.	Information	-
2.2	The system shall interface with network elements on one end and LIM (Lawful Interception and Monitoring) system at LEA ends over standard defined interfaces.	Information	-
2.3	**Description of Network Elements/Component** The general architecture for Lawful Interception and Monitoring System is shown in the figures given below	Information	-
2.4	**Definitions:**	Heading	-
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.	Information	-
2.4.2	**Monitoring:** Recording and storing of target subscribers' communications and communication related data by authorized Central and State Government agencies.	Information	-

2.4.3	**LEA:** Lawful Enforcement Agency of the Government authorized for seeking lawful interception.	Information	-
2.4.4	**LIS**: Lawful Interception System that is responsible for intercepting, correlating and transparently passing the CC and CRI/IRI 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.	Information	-
2.4.5	**LIM:** Lawful Interception and Monitoring System available at the LEA's.	Information	-
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.	Information	-
2.4.7	**Target Identity**: Technical identity (e.g. the interception's subjects directory number/IMS Information identity), which uniquely identifies a target of interception.	Information	-
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.	Information	-
3.0	**Functional/Operational Requirements**	Heading	-
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.	Information	-
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.	Check the Target assignment as per E.164 numbering plan/IMS Identity. Also Check the Part of "Calling Line Number" and "Part of Called Number" is targeted. Check the Interception data also, it should be based on the assigned target.	Fill from here
3.1.2 (i)	**Access to Communication Content (CC)** 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), Any combination of the above forms.	Interception capability should be checked for various types of communication as mentioned in the clause.	
3.1.2 (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.	Test No. 1	
3.1.3	**Access to Communication Related Information (CRI)**	Heading	-
(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)	Make different types of communications to and from a target and check the data as mentioned in	

	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.	the clause in the CRI/IRI. (Setup as per Test No. 1)	
(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.	Make Multiple Communication and verify this clause.	
(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	Verify this clause by checking GUI support. It should be checked for following, 1. Manual Provisioning 2. Electronic Provisioning To check LIID parameter used by LIS, it should be same as supplied in the electronic request from LIM in case of CMS.	
(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.	Invoke different supplementary services of the target and verify that all are reported to Law Enforcement Agency (LEA) as per ETSI standard ES 201 671 version 3.1.1 and it has no impact on the monitoring function and check that the corresponding parameters are present when the service is used. Check that when the target invokes various supplementary services	

		such as call waiting CFB, CFNR, CFU, MCT, CH, CONF etc, the monitoring centre is informed via CRI/IRI. Check various messages and parameter in which such information is given to LIM.	
(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	This clause is optional and verify when applicant applied for IP delivery also. Verify the Signalling which may be as per SIP, H.323 or other. Interception capability should be checked for various types of communication as mentioned in the clause.	
3.1.4	**Conditions of Access**	Heading	-
(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.	Verify that access to a target is supported in real time and for full time. CC and CRI/IRI is available at the monitoring centre immediately. In case of link failure, CRI/IRI is sent as soon as the link is restored. Record the time difference between origination of call and the transmission of CRI/IRI.	
(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.	**Information**	**-**
(iii)	The operation and services (basic & supplementary) of the target subscriber line shall not be affected in any manner.	Verify that the operation of the target subscriber shall not be affected by testing various types of calls from target.	
(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.	Verify this by making a multiparty call or conference call including target. Check that communication of all parties involved in the conference should be available.	

(v)	It shall be possible to carry out operations required for interception without any interruption to service.	Verify that different operations required for interception shall not affect the service if any.	
(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.	Verify that there is no change in the quality of a communication (speech level/data speed /Fax quality/noise online etc.) when the subscriber is targeted and when it is not targeted.	
(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.	Configure two LIM Providers (LEAs) with the LIS. Now a target is assigned for one LEA, then check & verify that Intercepted data (CC and CRI/IRI) is only sent to concern LEA.	
3.1.5	**Multiple and Simultaneous Monitoring**	Heading	-
3.1.5.1	Provision shall exist to monitor a single target subscriber simultaneously by at least TWELVE monitoring agencies.	Check that a single target could be provisioned for atleast 12 different agencies and could be simultaneously monitored by 12 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.	Verify that if a single target is provisioned for more than one agency than in such cases, each access is kept separate and distinct to others.	
3.1.6	**Encryption and Encoding**	Heading	-
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.	Check CC is transmitted in its original form.	
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.	Information	-
3.1.7	**Requirements of the Monitoring Equipment:**	Heading	-
(i)	The monitoring equipment shall support recording and storing the communication content and communication related information of at least 480 simultaneous calls. The number of activated targets shall be at least 3000.	Verify the capability of Monitoring equipment to support no. of simultaneous calls & no of activated targets. Traffic generator can be used to verify simultaneous capability. Note that CRI is sent for targets for which call Content is not sent because all the trunks towards mediation equipment are occupied because of other targets.	
(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.	Check the capability of Monitoring equipment for decoding.	

(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.	Verify this clause by making a FAX or data call.	
(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.	Check the indication of 'start of the call' and 'end of the call' at LIM in CRI/IRI.	
(v)	Monitoring equipment shall be capable receiving and storing the communication related information in the system disk for all the communication routed to it.	Verify the stored CRI/IRI information in a separate file in the disk.	
(vi)	Monitoring shall be possible for the entire duration of the communication without losing any part of telecommunications.	Verify this for the entire duration of the communication.	
(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.	Verify this clause.	
(viii)	The operation of the target subscriber line shall not be affected in any manner.	Covered in clause no. 3.1.4 (iii)	
(ix)	No indication whatsoever should be given to the target subscriber that intercept function has been invoked on the target.	Verify that no indication is noted in following different situation; 1. Successful provisioning 2. Unsuccessful provisioning 3. Other O&M person 4. no indication in the CRM module of target 5. no indication at target	
(x)	The monitoring shall not affect the basic and supplementary services of the subscribers under monitoring.	Verify basic supplementary services by dialing them from target subscriber.	
(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.	Verify that the system is able to support the conversion of intercepted data in a readable and audible format and is able to support the storage of the intercepted data on DVD/CD disks 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.	Verify these two modes supported by monitoring center supported by monitoring center..	
(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.	Verify various tools supported by monitoring center. (Take the complete list of supported functions from vendor and verify them)	
(xiv)	The text search implementation shall be sensitive to misspelling of keywords, grammatical extension of keywords apart from basic string matching capabilities.	Verify this.	
(xv)	The online filtering shall be activated based on single/multiple call	Verify the activation of	

	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.	online filtering in various scenario.	
(xvi)	The monitoring centre shall support both dynamic and static allocation of time slot for the purpose of call content delivery.	Verify dynamic and static allocation of time slot.	
3.1.8	**System supervision**	Heading	-
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.	Verify this clause.	
3.1.8.2	The equipment shall provide for print-outs and visual/audible alarms to assist in efficient administration.	Verify this clause.	
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.	Verify this clause.	
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.	Take undertaking from the applicant.	-
3.1.9	**Maintenance facilities**	Heading	-
3.1.9.1	The system shall have the capability to monitor its own performance and to detect, analyze, locate, and report faults.	Verify that the system have the capability to monitor its own performance.	
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.	Information	-
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.	Information	-
3.1.10	**Diagnostic capabilities**	Heading	-
(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.	Take the list/details of Online and of off-line diagnostic programs. And also the procedure for invoking such program and the procedure for consulting fault dictionary.	
(ii)	All the hardware testers necessary for efficient maintenance of the system shall be provided. Details of the testers shall be indicated.	Take the list of testers required for maintenance and verify it.	
(iii)	The test procedures, recommended for efficient maintenance of the system, shall be indicated. This shall include details of the testes, their periodicity, etc.	Take details of test procedures & check it.	
(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.	Verify this clause by giving some wrong command for creating malfunctioning and then check a fault message or alarm and its details. This detail should contain the rectification procedure. Take the list of classification of all alarms and check.	
(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.	Verify this clause and also check the provision to extend the alarm.	
3.1.11	**Storage**	Heading	-
(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	Verify that the detail for the calculation of disk capacity is provided by the	

	disk capacity.	supplier.	
(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.	Verify the storage of CC.	
(iii)	The equipment shall be capable of storing at least 2000 hours of 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.	Verify this clause.	
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.	(i) Verify that the communication content reaches to the operator at monitoring position in real-time for a target specified for him. (ii) Verify that the communication content for each target is stored in a separate area. And can be retrieved and presented target-wise and date-wise to the operator whenever requested through man-machine commands. (iii) Undertaking from the applicant.	
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 $\pm$ 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.	Check the type of power supply. Under taking required.	
3.1.14	**HARDWARE REQUIREMENTS**	Heading	-
(i)	Compact and high-performance state-of-the-art hardware shall be used.	Information	-
(ii)	The hardware platform shall be open-ended and modular in architecture so that the equipment can be augmented and adapted to customer requirements.	Under taking required	-
(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.	Under taking required	-
(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.	Verify this clause by checking the redundancy of any subsystem. Choose a sub-system which has redundancy. Now create some fault or remove running sub-system and check. This does not affect the performance and feature	

		of 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.	Under taking required	
(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.	Verify this clause. Remove or create some fault into running/active processing sub-system and check that the standby processor is now active automatically with zero downtime.	
3.1.15	**SOFTWARE REQUIREMENTS**	Heading	-
(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.	Under taking required	-
(ii)	The normal operation shall not be affected while undertaking software updates, enhancement of features or correction to programs.	Under taking required	-
(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.	Under taking required for (a) (b) and (c) Verify the clause (d) (e) and (f). (software should have sufficient checks to monitor the correct functioning of the system. Test programs should have fault tracing for detection and localization of system faults. automatic system reconfiguration should be happened 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.	Under taking required	-
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).	Under taking required	-
4.0	**Interface Requirements**	Heading	-
4.1	**Interfaces between mediation equipment and monitoring equipment:**	Heading	-
4.1.1	**Interface for transmission of communication content**	Heading	-
(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 133 107 & 133 108 in IMS scenario and as per ETSI 101 671 / 102 232-5 standard in PSTN/NGN scenario)	Verify this clause. Check all PCM links of 2048 kbps at system console. For 12 monitoring agency, it should be at least 24 PCM links (2 for each LEA). Also verify the physical port on the system corresponding to the PCM.	
(ii)	Signalling: The Signalling between the mediation equipment and the monitoring equipment shall be one of the following:	Verify the signaling between mediation &	

	• 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.	monitoring equipment. (Check IAM message in case of CCS7 and SETUP message in case of PRI) Check also IP delivery.	
(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.	Verify this clause.	
(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	Verify this clause.	
4.1.2	**Interface for Transmission of Communication related information:**	Heading	-
(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 be TCP/IP protocol using FTP/SFTP for data transfer.	Verify the TCP/IP protocol using FTP/SFTP for data transfer in this clause.	
(ii)	The data transfer protocol for receiving the call related information between monitoring equipment and mediation equipment shall be compatible.	Check the compatibility of data transfer protocol.	
(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.	Verify this clause.	
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.	Verify this clause when both CC & CRI/IRI are combined and sent.	
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 1×10^{-9} per day.	Test no. 2	
4.3	**Slip:** Under synchronized condition, slip observed on the PCM links shall be less than or equal to 2 slips in 24 hours.	Test no. 3	
4.4	**Selection of priority :** Equipment shall be capable of selecting the input timing reference depending on the pre-set priority.	Check of priority for clock inputs which should include 2Mb/s and 2Mhz references: **a)** The equipment should be synchronised with the first priority reference. Other two references also shall be connected. **b)** The timing reference should be removed and it should be checked that the next priority reference is now used for synchronisation.	

<table>
<tr><td></td><td></td><td>c) Step (b) should be repeated with all available references.
After the equipment goes in the holdover mode, one of the timing references should be restored. It should be checked that the restored timing reference is used for synchronisation automatically.</td><td></td></tr>
<tr><td>4.5</td><td>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:
<table>
<tr><th>Frequency</th><th>Jitter Amp to be applied Peak to Peak (UI) **</th><th>Status of Exchange clock</th></tr>
<tr><td>20 Hz</td><td>1.5</td><td>Synch mode</td></tr>
<tr><td>2.4 KHz</td><td>1.5</td><td>--do--</td></tr>
<tr><td>18 KHz</td><td>0.2</td><td>--do--</td></tr>
<tr><td>100 KHz</td><td>0.2</td><td>--do--</td></tr>
</table>
** For 2048 Kbps 1 UI = 488 ns.</td><td>Test no. 4</td><td></td></tr>
<tr><td>4.6</td><td>Traffic statistics: Traffic report shall be generated by the equipment for each PCM link separately.</td><td>Verify that the Traffic report is generated by the equipment for each PCM link separately.</td><td></td></tr>
<tr><td>4.7</td><td>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.</td><td>Test no. 5</td><td></td></tr>
<tr><td>4.8</td><td>Group delay: Group delay shall meet the following requirements:
<table>
<tr><th>Frequency (Hz)</th><th>Permitted limit (micro seconds)</th></tr>
<tr><td>500</td><td>900</td></tr>
<tr><td>604</td><td>900</td></tr>
<tr><td>1000</td><td>900</td></tr>
<tr><td>1792</td><td>900</td></tr>
<tr><td>2604</td><td>900</td></tr>
<tr><td>2792</td><td>900</td></tr>
</table>
Note: 900 micro seconds is the mean value. However, the limit for 0.95 probability of not exceeding is 1500 micro seconds.</td><td>Test no. 6</td><td></td></tr>
<tr><td>5.0</td><td>Quality Requirements</td><td>Heading</td><td>-</td></tr>
<tr><td>5.1</td><td>Qualitative Requirements (QR):</td><td>Heading</td><td>-</td></tr>
<tr><td>5.1.1</td><td>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.</td><td>Undertaking required</td><td>-</td></tr>
<tr><td>5.1.2</td><td>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.</td><td>Undertaking required</td><td>-</td></tr>
<tr><td>5.1.3</td><td>The failure of any component/subsystem in the system shall not result in the failure of complete system.</td><td>Verify the clause.</td><td></td></tr>
<tr><td>5.1.4</td><td>List of all components for which second source is not available should be provided.</td><td>List from applicant</td><td>-</td></tr>
<tr><td>5.2</td><td>Reliability and quality of service:</td><td>Undertaking required.</td><td>-</td></tr>
</table>

	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**	Report from Accredited test lab along with certificate from lab	
7.0	**Safety Requirements**	A test certificate and test report shall be furnished from a test agency which shall be ISO 17025accredited agency.	
8.0	**Security Requirements**	Heading	-
8.1	**Security aspects**	Heading	-
8.1.1	Secure data network arrangements shall be provided between monitoring Centre and the exchange for the intercept function commands.	Undertaking required.	-
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.	Verify the clause.	
8.1.3	The authorized user of the LEA shall be able to start the target synchronization process manually, whenever necessary.	Information	-
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.	Undertaking required	-
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.	Verify the clause	
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.	Verify the clause	
8.1.7	Suitable safeguards for security of Mediation Equipment like protection from public domain, safe retention of information/data/observation shall be there.	Undertaking required	-
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.	Verify the clause	
8.1.9	The system shall support secure reception of data on IP interface using IP-SEC.	Verify the clause	
8.1.10	The system shall support encryption between mediation equipment and monitoring centre.	Verify the clause	
8.1.11	The system shall have provision for protection against viruses, worms and other vulnerabilities / threats with regular updates.	Undertaking required	-
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.	Verify the clause	
9.0	**OTHER MANDATORY REQUIREMENTS**	Heading	-
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.	Information	-
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.	Verify the clause	

	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	Verify the clause	
9.1.3	Access to all MML commands related to line interception and monitoring shall be controlled through a multi-level password mechanism.	Verify the clause	
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.	Verify the clause	
9.1.5	Hand over interface for target administration shall be supported, if required by the service provider.	Verify the clause	
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.	Verify the clause	

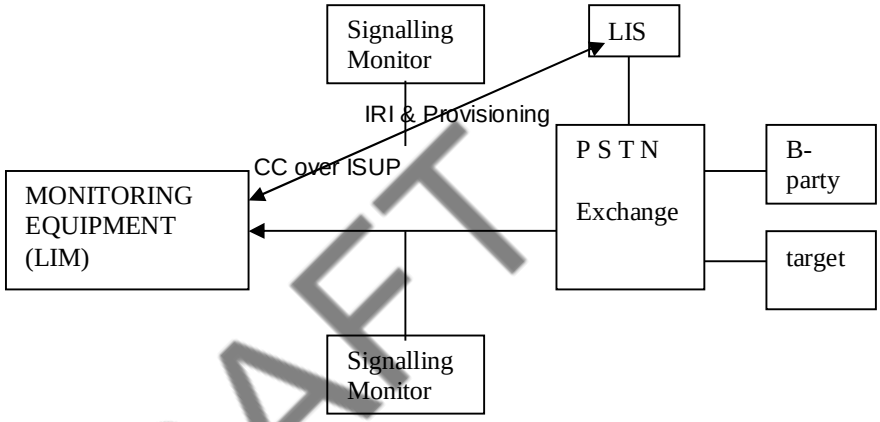
** Physical Check/Declaration/Documentation/ Report from Accredited test lab/ Functional verification / Information / Test No.*

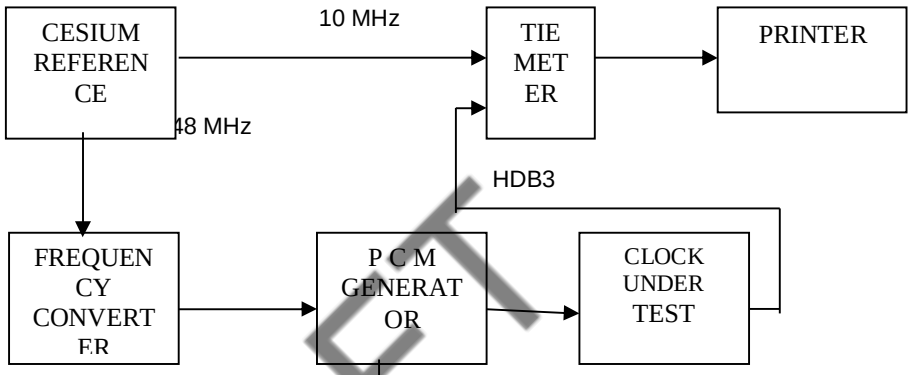
I. TEST SETUP & PROCEDURES:

Note :

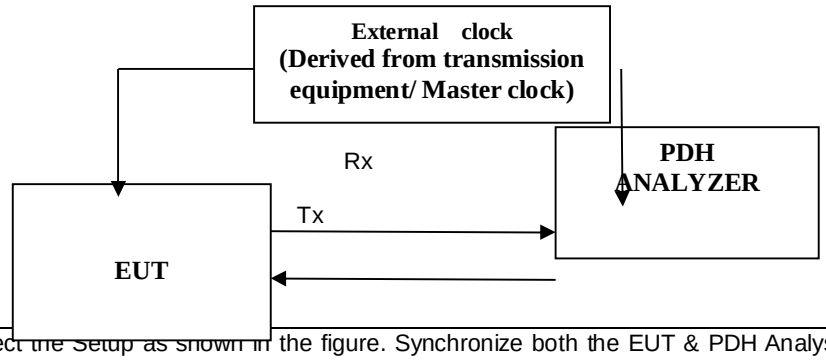
(a) The test set-up given in this document are tentative and may be changed by testing officer, taking in to account, network/testers/ analyzer/simulator availability. In case of any discrepancy between this TSTP and GR, GR clause shall prevail.

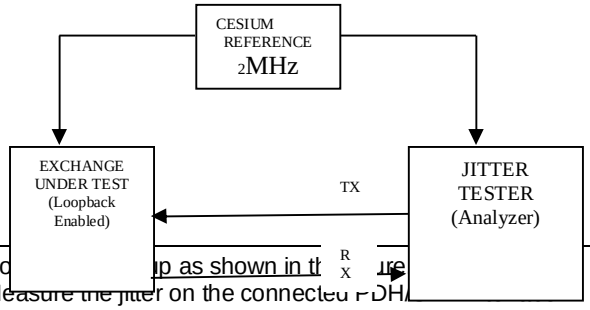
(b) Where, it is not possible to conduct the test with public network exchange/ system or main exchange connectivity is not available, simulator or any switching node may be used for testing purpose.

Test No.	1
Test Details	Signalling Message / ISUP Message
Test Instruments Required	1. Signalling Monitor
Test Setup	
Test Procedure	1. Capture/observe Signalling flow by signalling Monitor. 2. Check ETSI correlation parameters LIID, CID & CCLID.
Test Limits	ETSI correlation parameters as per ETSI TS 101 671 & TS 101 232.
Expected Results	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.

Test No.	2
Test Details	Clause no. 4.2 (Test for Measurement of Frequency Stability in Holdover Mode)
Test Instruments Required	TIE Meter (PDH Analyzer)
Test Setup	
Test Procedure	1. Connect the Setup as shown in the figure. 2. Measure the TIE using the TIE Meter for 24 Hrs. 3. calculate stability ar range. Synchronise the exchange a ithout any jitter by clock. After the exchange is synchr lised, introduce the jitter in the reference input. Increase jitter amplitude upt Hz. If the jitter amplitude is increased further, exchange clock will reject th will go to holdover mode. The input reference should be removed and the TIE measurement in holdover mode should be started at this point for 24 Hrs. Clock stability should be calculated as follows: Clock stability= Time Interval Error (TIE)/Measurement Duration
Test Limits	Minimum Stability of clock in Holdover Mode should be better than 1* 10E-9

Test No.	3
Test Details	Clause 4.3 (Slip Rate)
Test Instruments Required	PDH Analyzer

Test Setup	
Test Procedure	1. Connect the Setup as shown in the figure. Synchronize both the EUT & PDH Analyser (Testing equipment) as per test setup from external timing reference which may be extracted from transmission equipment.) 2. After the EUT is synchronised and stabilized, run the measurement (PRBS bit pattern) which should be started at this point for 96 Hrs. 3. Measure Slip on PDH analyzer for a period of at least 96 hours of operation. In synchronised mode of operation, not more than 2 slips per day are permitted.
Test Limits	Under synchronized condition, slips observed at the given interface of EUT shall be less than or equal to 2 slips in 24 hours.

Test No.	4
Test Details	Clause no. 4.5 (Test for Jitter Tolerance at input port)
Test Instruments Required	PDH/SDH Performance Analyser or Jitter Tester
Test Setup	
Test Procedure	1. Co… up as shown in th… re 2. Measure the jitter on the connected PDH/… 3. Verify whether the jitter is within the tolerance limits. i) The jitter tolerance of the synchronisation equipment is measured as the maximum jitter amplitude, it can tolerate at the input, without losing synchronization ii) Measure the jitter tolerance of the synchronisation equipment by varying the amplitude and frequency of the input jitter for digital rate 2048 kbps.

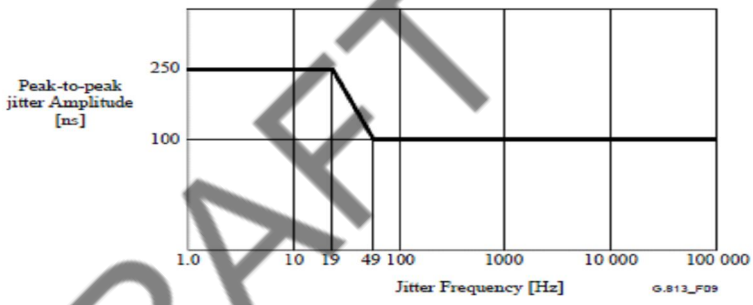
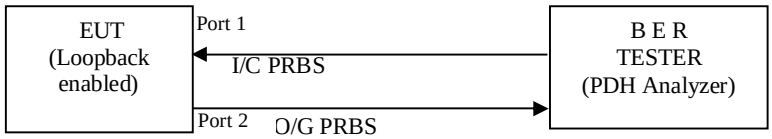
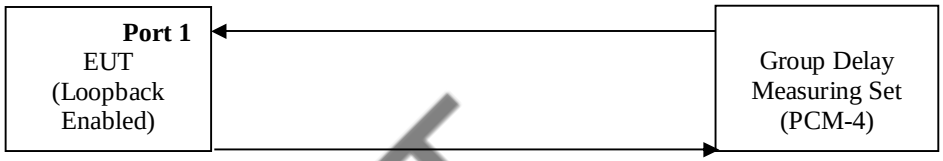
<table>
<tr><td>Test Limits</td><td>As per ITU T</td></tr>
<tr><td>Expected Results</td><td>Jitter tolerance at input port of 2048 kbps card as per ITU-T Table 16/G.823, as below
<table>
<tr><th>Frequency</th><th>Jitter amplitude to be applied - Peak to peak (UI)</th><th>Status of Exchange clock</th></tr>
<tr><td>20 Hz
2.40 KHz
18 KHz
100 KHz</td><td>1.5
1.5
0.2
0.2</td><td>Synch mode
“
“
“</td></tr>
<tr><td colspan="3">Note 1: For 2048 kbps rate 1 UI = 488 ns.
Note 2: Synchronisation should not fail with the above input Jitter at various frequencies.</td></tr>
</table>
Jitter tolerance at input port of 2048 khz/ synchronisation card : The lower limit of maximum tolerable input jitter for 2048 kHz and 2048 kbit/s signals carrying synchronization to a SEC is given in Figure 9 of ITU-T G.813.


Figure 9/G.813 – Lower limit of maximum tolerable input jitter</td></tr>
</table>

<table>
<tr><td>Test No.</td><td>5</td></tr>
<tr><td>Test Details</td><td>Clause 4.7 - Bit Error Ratio</td></tr>
<tr><td>Test Set up</td><td> 
</td></tr>
<tr><td>Test Procedure</td><td>1. Connect the Setup as shown in the figure.
2. Measure the BER using the BER tester for 48 Hrs. Also measure PRBS loss, if any
3. Check whether the BER is within limits as per clause</td></tr>
<tr><td>Test Result</td><td>BER measurement should be made for a period of 48 hours of operation. Measured BER should be better than 1 in 10^9 for a 64 kb/s connection through the switch.</td></tr>
</table>

Test No.	*6*
Test Details	*Clause no. 4.8 (Group Delay)*
Test Instruments Required	*PCM Channel Measurement Set/ PCM -4*
Test Setup	
Test Procedure	*1. Connect the Setup as shown in the figure.* *2. Measure the group delay using the PCM-4 for digital to digital interface.* *3. Check whether the values within the specified limis*
Test Limits	*As per the table mentioned below*
Expected Results	**Measurement of Group delay between Digital to Digital Interfaces**

Frequency Hz	**Group delay between Digital to Digital Interfaces Permitted limit (micro sec)**
500	900
604	900
1000	900
1792	900
2604	900
2792	900
Note : 900 micro sec is the mean value. However, the limit for 0.95 probability of not exceeding is 1500 micro sec.	

J. SUMMARY OF TEST RESULTS

GR/IR No._____

TSTP No._____

Equipment name & Model No._____

Clause No.	***Compliance*** *(Complied /Not Complied / Submitted/Not Submitted / Not Applicable)*	***Remarks / Test Report Annexure No.***

[Add as per requirement]

Date:

Place: ***Signature & Name of TEC testing Officer /***

**** Signature of Applicant / Authorized Signatory***

**** Section J as given above is also to be submitted by the Applicant/ Authorised signatory as part of in-house test results along with Form-A. The Authorised signatory shall be the same as the one for Form 'A'.***