सत्यमेव जयते

अनंतिम टेस्ट गाइड

टीईसी ४९०२१: २०२५

(पूर्व सं: टीईसी/आई टी/आईपी एल सी- ०१/०१ जुलाई २००७)

PROVISIONAL TEST GUIDE

TEC 49021:2025

(Earlier No. : TEC/IT/IPLC-01/01 JUL 2007)

For

इंटरनेशनल प्राइवेट लीज्ड सर्किट (IPLC) ट्रैफिक लॉफुल इंटर्सेप्शन एंड मॉनिटरिंग सिस्टम (IPLC-TLMS)

International Private Leased Circuit (IPLC) Traffic Lawful Interception and Monitoring System (IPLC-TLMS)

(जीआर सं: टीईसी ४९०२०: २०२५)

(Standard No.: TEC 49020:2025)

ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र
खुर्शीदलालभवन, जनपथ, नई दिल्ली–११०००१, भारत

TELECOMMUNICATION ENGINEERING CENTRE
KHURSHID LAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA

www.tec.gov.in

Release 02: XXX, 2025

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 Test Guide of testing pertains to Test Schedule and Test procedures for **International Private Leased Circuit (IPLC) Traffic Lawful Interception and Monitoring System (IPLC-TLMS)**.

CONTENTS

A. INTRODUCTION

This document enumerates detailed test schedule and procedure for evaluating conformance/functionality/ requirements/ performance of the **International Private Leased Circuit (IPLC) Traffic Lawful Interception and Monitoring System (IPLC-TLMS)**

to be deployed-in or implemented through Indian Telecom Network.

B. HISTORY SHEET

Sl. No.	Standard No.	Title	Remarks
1.	TEC/IT/IPLC-01/01 JUL 2007	TSTP for IPLC-TLMS	Issue No. 1
2.	TEC 49021:2025	Test Guide for IPLC-TLMS	Incorporating the updations done in the GR 49020:2025

C. General information:

Sl. No.	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)*

S No.	Name	Designation	Organization	Signature
1.				
2.				

E. List of the Test Instruments:

S No.	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			

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.: -

Cl. No	Sub Cl.	Clause	Type of Test	Compliance
			Physical Check / Declaration / Documentation/ Report from Accredited Test Lab / Functional Verification / Information / Lab Test (Test Reference)	**Complied / Not Complied / Submitted / Not Submitted / Not Applicable (Indicate Annexure No for Test Results)**
1.0		Introduction	Information	
	1.0.1	International Long Distance (ILD) Service Providers are offering International Private Leased Circuits (IPLCs) to customers. Hence, there is a need to put in place a lawful interception and monitoring system for intercepting and monitoring the IPLCs, so as to determine the type of traffic and to know the contents of the traffic passing over the IPLCs.	Information	
	1.0.2	This document covers the Generic Requirements of Lawful Interception and Monitoring System (IPLC-LIMS) for IPLC traffic for the purpose of lawful interception and monitoring of IPLC traffic in near real time by authorised Law Enforcement Agencies (LEAs).	Information	
	1.0.3	The scope of the IPLC-LIMS is to intercept and monitor the information carried on the IPLC, which may be Voice/Data traffic. The IPLC-LIMS can also be used for ISP Gateways.	Information	
1.1		IPLC-LIMS	Information	
	1.1.1	The IPLC-LIMS shall intercept IPLC traffic by providing access to and delivery of the targeted IPLC's Traffic Content (TC) and the Intercept Related Information (IRI) based on the interception criterion as given in clause 2.1 of this document, in near real time to Authorized Law	Declaration	

		Enforcement Agencies (LEAs).		
	1.1.2	The IPLC-LIMS shall also monitor IPLC traffic by providing recorded/stored and post processed intercepted data to authorised Central and State Government Law Enforcement Agencies. The architecture of IPLC-LIMS shall be as per Fig. 1. The IPLC-LIMS shall consist of two functional components:	Declaration Refer GR IPLC	
	1.1.2 (i)	IPLC Lawful Interception System (IPLC-LIS), which shall be deployed at the ILD Centres for intercepting the IPLC traffic on individual IPLC and egress point(s) of international bandwidth from India and it shall be used for interception of the IPLC traffic based on interception criterion.	Declaration	
	1.1.2 (ii)	IPLC Lawful Monitoring System (IPLC-LIM), which shall be deployed at the Monitoring Centre (MC), for monitoring of targeted IPLC's traffic and related information by providing recorded/stored and post processed intercepted data as per the requirement.	Declaration	
	1.1.3	IPLC-LIMS, therefore, needs to perform the full range of tasks necessary to intercept and monitor the required IPLC traffic accurately and securely. The basic tasks of the proposed IPLC-LIMS shall include the following:	Functional verification	
	1.1.3 (i)	Target management to activate and deactivate targets based on interception criteria.	Functional verification	
	1.1.3 (ii)	Collecting intercepted data for the assigned target(s).	Functional verification	
	1.1.3 (iii)	Delivering intercepted data to the Monitoring Centre in a secured way.	Functional verification	
	1.1.3 (iv)	Post processing of intercepted data like building of web-page/ session etc.	Functional verification	
	1.1.3 (v)	Controlling system security, monitoring and maintaining system activity.	Functional verification	
	1.1.3 (vi)	Exporting and Viewing of intercepted information.	Functional	

			verification	
	1.1.3 (vii)	MIS Report generation.	Functional verification	
	1.1.3 (viii)	Purging of old data which is no more required after deactivation of target(s).	Functional verification	
	1.1.3 (ix)	The target administration through an electronic interface by authorized agencies of Govt. on request from authorized agencies.	Functional verification	
	1.1.4	Link between LIS Gateway Locations & Central backend of the service provider should have sufficient bandwidth & 99.99% availability, so that no intercepted data is lost. The requirement of bandwidth for IPLC-LIMS i.e. for connectivity between IPLC-LIS and IPLC-LIM shall be specified by purchaser.	Functional verification	
	1.1.5	The IPLC-LIMS shall have capability of generating unique Acknowledgement Number for each request received for interception. It shall also assist in generating the acknowledgement to the authority in a secure manner, on request by issuing an operator command. (There should not be any connectivity of LIS/LIM with internet or no details regarding lawful interception should be passed through internet/public channels. Hence other secure modes of sending acknowledgement may be used.)	Functional verification	
	Technical Requirements of IPLC Traffic Lawful Interception System (IPLC-LIS)			
2.0		**IPLC Traffic Lawful Interception System (IPLC-LIS)** shall consist of following components as detailed below:	Declaration	
	2.0 (a)	**Probe:** This can be either hardware or software emulated functional entity deployed/ configured at the interception points to intercept the IPLC traffic. It shall be installed at various interfaces to be monitored in IPLC network to collect the target traffic. The Taps with the minimum insertion loss shall be used. The figure for the insertion loss like 90:10 or 80:20 etc. shall be indicated by Tendering Authority.	Functional verification (Refer Annex. I GR IPLC)	

	2.0 (b)	**Traffic Aggregator**: It shall be installed at each of interception points or at a common site for a group of interception points for aggregating the traffic from different probes. The traffic aggregator shall communicate with the Monitoring centre at IPLC-LIM for sending the intercepted traffic in a secure way and using delivery standards as per ETSI.	Functional verification	
2.1		**Probe**	Information	
	2.1.1	The Probe in IPLC-LIS is a hardware and/or software entity to intercept the IPLC traffic and send the intercepted data to an Aggregator, which either stores it or forwards it to IPLC-LIM.	Information	
	2.1.2	The Probe may be in any combination of the following forms:	Declaration	
	2.1.2 (i)	wiretap/Optical tap/splitter providing a copy of data being carried on an interface	Functional verification	
	2.1.2 (ii)	functional module in the Networking Equipment like Router, RAS (Remote Access Server), LAN (Local area network) Switch, etc. providing a copy of the data flowing through the networking equipment.	Functional verification	
	2.1.2 (iii)	device plugged in parallel to an interface and configured for intercepting the data.	Functional verification	
	2.1.2 (iv)	device plugged in SDH- Digital Cross Connect using Continue and Drop facility.	Functional verification	
		The types and number of probes shall be indicated by Tendering Authority.	Refer Annex. I GR IPLC	
	2.1.3	The Probe shall be placed on suitable places for intercepting all targets specified in clause 2.1.9.	Declaration	
	2.1.4	The Probe shall have the capability of intercepting the IPLC traffic on any one or a combination of the following interfaces by Tendering Authority.	Functional verification (Refer Annex. I GR IPLC)	
	2.1.4 (i)	E1 interface as per ITU-T Recommendation G.703. The probe shall be capable of being configured to intercept	Functional verification	

		traffic being carried in any combination of timeslots.		
	2.1.4 (ii)	E3 interface as per ITU-T Recommendation G.703. The Probe shall be capable of being configured to intercept traffic being carried in any of the E1s and also any combination of timeslots in that E1.	Functional verification	
	2.1.4 (iii)	STM-1 interface as per ITU-T Recommendation G.703 or G.783. The probe shall be capable of configuration to intercept any of the E1 being carried in the SDH Container. It shall also be capable of being configured to intercept the traffic being carried in any group of the time slots of any E1 channel in SDH container. The probe in this case shall be remotely manageable from the Central NMS.	Functional verification	
	2.1.4 (iv)	45 Mbps as per ITU-T Recommendation G.703.	Functional verification	
	2.1.4 (v)	STM-16 Optical interface mono-mode/Long haul/short haul.	Functional verification	
	2.1.4 (vi)	10/100 Mbps Auto sensing Ethernet as per IEEE 802.3.	Functional verification	
	2.1.4 (vii)	STM-64 Optical Interface mono-mode/long haul/ short haul.	Functional verification	
	2.1.4 (viii)	STM 256 Optical Interface mono-mode/ long haul/ short haul.	Functional verification	
	2.1.4 (ix)	400G/ 400GbE autosensing Ethernet as per IEEE P802.3bs.	Functional verification	
	2.1.4 (x)	800G/800GbE autosensing Ethernet as per IEEE P802.3df	Functional verification	
	2.1.4 (xi)	Probes should support 10 Gbps/ 100 Gbps/400 Gbps/800 Gbps and above Ethernet Bandwidth.	Functional verification	
	2.1.4 (xii)	OTU2/OTU4 interface.	Functional verification	

	2.1.5	Different protocols shall be allowed to be aggregated to a router or directly supported by the IP-Probe. The Analysis server(s) shall be able to decode, analyse and reconstruct the following protocols (latest versions).	Functional verification	
	2.1.5 (i)	HDLC	Functional verification	
	2.1.5 (ii)	PPP including encryption and compression	Functional verification	
	2.1.5 (iii)	Frame Relay	Functional verification	
	2.1.5 (iv)	AAL5 - ATM	Functional verification	
	2.1.5 (v)	X.25	Functional verification	
	2.1.5 (vi)	SNA	Functional verification	
	2.1.5 (vii)	IP (IP address)	Functional verification	
	2.1.5 (viii)	TCP (frames with minimum errors, sorted sequentially according to connection or port number).	Functional verification	
	2.1.5 (ix)	UDP (frames sorted sequentially according to connection or port number).	Functional verification	
	2.1.5 (x)	Email (POP3 [incoming messages], SMTP [outgoing messages], IMAP4 [incoming messages, mail and folder lists]).	Functional verification	
	2.1.5 (xi)	MIME [formats and encoding].	Functional verification	
	2.1.5 (xii)	RADIUS	Functional verification	
	2.1.5 (xiii)	Chat and Instant Messaging atleast (IRC [Chat and file transfer over IRC], Microsoft Messenger [Messenger via Server, Text and nick names], Yahoo Messenger [Messenger via Server, Text and nick names], AOL	Functional verification	

		Messenger [Messenger Peer-To-Peer and via Server, File transfers, Text and nick names], ICQ [Messenger via Server, Text and nick names])		
	2.1.5 (xiv)	AOL Access 5.0, 6.0, 7.0 (ISP access and TCP/IP protocols such as HTTP and FTP excluding AOL proprietary protocols such as email)	Functional verification	
	2.1.5 (xv)	AOL mail 5.0 (Incoming/Outgoing emails and attachments)	Functional verification	
	2.1.5 (xvi)	HTTP Version 1.0, 1.1 (XML, HTML) [Web pages, downloads, uploads, compression]	Functional verification	
	2.1.5 (xvii)	FTP/TFTP (full session transcript, details, summary and transferred files)	Functional verification	
	2.1.5 (xviii)	Telnet (Transferred communication)	Functional verification	
	2.1.5 (xix)	NNTP (Messages and folder list)	Functional verification	
	2.1.5 (xx)	SIP	Functional verification	
	2.1.5 (xxi)	Voice-over-IP (ITU-T H.323, H.248, G.711, G.722.2, G.723.1, G.726, G.728, G.729AB, AMR, SIP)	Functional verification	
	2.1.5 (xxii)	RTP/RTCP	Functional verification	
	2.1.5 (xxiii)	Lotus Notes	Functional verification	
	2.1.5 (xxiv)	WAP (Wireless Application Protocol) for SMS, GPRS and MMP	Functional verification	
	2.1.5 (xxv)	Video over IP (H.263, H.264)	Functional verification	
	2.1.5 (xxvi)	Encrypted IP traffic – (extraction of GPS location, MSISDN, IDFA, Username and Persistent Cookie, credentials (usernames/passwords), host, service, SSL	Functional verification	

		version, identifier and username, IP address and subscriber device details (model, OS and browser) from clear data leaks from encrypted applications traffic when such data is available.)		
		The tendering authority may define the actual protocol support requirements	Refer Annex. I GR IPLC	
	2.1.6	The Probe shall stealthily intercept the IPLC traffic without revealing its identity. The operation and services of the targeted IPLC subscriber shall not be affected in any manner.	Functional verification	
	2.1.7	The interception shall be implemented in such a way that neither the targeted IPLC subscriber(s) nor any other unauthorized person gets any indication whatsoever that intercept function has been invoked.	Functional verification	
	2.1.8	The system shall support the privacy of non-targeted user's remains intact at all times and interception is effected for the targeted users only.	Functional verification	
	2.1.9	IPLC-LIS shall have access to the entire content transmitted or caused to be transmitted to and from the targeted IPLC in near real time and shall be capable of intercepting the following IPLC traffic along with the relevant IRI:	Functional verification	
	2.1.9 (i)	Data traffic including the Internet traffic (HTTP, e-mail, FTP etc)	Functional verification	
	2.1.9 (ii)	Voice or Data including SMS, GPRS, CDMA or MMS traffic that may appear over the Channelised links, including analysis of the following out-of-band and in-band signaling:	Functional verification	
	(ii- a)	PRI as per as per latest TEC standard on PRI available on TEC website.	Functional verification (Refer TEC Website)	
	(ii- b)	R2MFC (Indian) as per latest TEC standard on R2MFC available on TEC website.	Functional verification	

			(Refer TEC Website)	
	(ii- c)	SS7 including MAP as per latest TEC standard on SS7 available on TEC website.	Functional verification (Refer TEC Website)	
	2.1.9 (iii)	Voice-over-IP (ITU-T H.323, H.248, G.711, G.722.2, G.723.1, G.726, G.728, G.729AB, MPEG4), SIP.	Functional verification	
	2.1.9 (iv)	Fax including Fax over IP (ITU-T T.37, T.38)	Functional verification	
	2.1.9 (v)	Video including Video over IP (ITU-T H.261, H.263, H.264, VP9, H.265/HEVC, AV1, H.266/VVC, GSM 06.10)	Functional verification	
	2.1.9 (vi)	Encrypted data record (EDR)	Functional verification	
	2.1.9 (vii)	Crypto transactions in the Blockchain.	Functional verification	
	2.1.9 (viii)	Any combination of the above forms	Functional verification	
	2.1.10	The system shall be capable of intercepting the target(s), whose definition shall be done from the IPLC-LIM by the Operators on receipt of request from the competent authority and whose traffic is to be intercepted and monitored, by any combinations of the following parameters:	Functional verification	
	2.1.10(i)	MAC address of the actual physical device	Functional verification	
	2.1.10(ii)	Source and Destination IP address (IP version 4 and IP version 6)	Functional verification	
	2.1.10(iii)	TCP and UDP Port number	Functional verification	
	2.1.10(iv)	E-mail address in SMTP (Simple Message Transfer Protocol), POP3 (Post Office Protocol version 3), IMAP4 (Internet Message Access Protocol version4) [To, From, Copy to]	Functional verification	

	2.1.10(v)	POP3, IMAP4 Username	Functional verification	
	2.1.10(vi)	RADIUS (Remote Authentication Dial-In User Service), AAA and DHCP Username [Login-id]	Functional verification	
	2.1.10(vii)	RADIUS CLI (Caller Line Identification)	Functional verification	
	2.1.10(viii)	URL (Universal Resource Locator) address	Functional verification	
	2.1.10(ix)	Threshold for a type in a connection i.e. a PPP session or a leased line with percentage TCP, UDP, SCTP, etc. traffic more than a specified value	Functional verification	
	2.1.10(x)	Traffic Content dependent targets (e.g. a particular keyword in http, email etc or chat traffic and scanning the relevant text after protocol decoding)	Functional verification	
	2.1.10(xi)	User groups (e.g. Yahoo user groups)	Functional verification	
	2.1.10(xii)	Web mail (To, From, Copy to)	Functional verification	
	2.1.10(xiii)	IM ID (Instant Messaging Identity)	Functional verification	
	2.1.10(xiv)	Phone Number /VOIP Phone Number	Functional verification	
	2.1.10(xv)	Subnet address	Functional verification	
	2.1.10(xvi)	Leased Line (Circuit/ Channel number)	Functional verification	
	2.1.10(xvii)	X.25 address	Functional verification	
	2.1.10(xviii)	ATM/Frame Relay address	Functional verification	
	2.1.10(xix)	Mobile-GSM/CDMA Number (Called and Calling Party) for SMS, GPRS & MMS	Functional verification	
	2.1.10(xx)	Any combination of above including Boolean conditions	Functional	

		(AND, OR, ~~NOT~~ etc.) for above.	verification	
	2.1.10(xxi)	Mobile - GSM/CDMA Number (Called and Calling Party) for App based voice/video calls, Chats and other App based communication	Functional verification	
	2.1.10(xxii)	Keyword search for any specified target(s) in file transmitted In plain text file, pdf, MS word(.doc & .docx), MS Excel (.xls & .xlsx), MS PPT (.ppt & .pptx), etc.	Functional verification	
	2.1.11	The following target grouping rules shall be possible for the purpose of interception of IPLC traffic:	Functional verification	
	2.1.11 (i)	Packets originating from or destined to an IP - Sub-network.	Functional verification	
	2.1.11 (ii)	Packets between two specific IP – Sub-network .	Functional verification	
	2.1.11 (iii)	Packets destined to a specific IP address (client or server) and port range.	Functional verification	
	2.1.11 (iv)	Packets originating from a specific IP address (client or server) and port-range.	Functional verification	
	2.1.11 (v)	All frames between two MAC IDs.	Functional verification	
	2.1.12	Interception shall be possible for required duration of connection without loosing any part of traffic. However in case of keyword based interception the duration shall start after the spotting of the keyword(s).	Functional verification	
	2.1.13	Probe shall buffer those traffic content which are having readable characters (ASCII, Unicode, etc.) for at least 30 mins, so that when there is a keyword match, the whole message can be recreated from buffered data (Exact requirement for Probe buffering to be defined by tendering authority)The Probe shall send the IPLC's intercepted traffic directly to the Traffic Aggregator in near real time over standard interface like Ethernet/ Fast Ethernet as per IEEE 802.3 or Gigabit Ethernet interface Aggregator without any de cryption/ decoding/ any other modification.	Functional verification	

	2.1.14	The IPLC TC and relevant IRI shall be provided in a way that allows for accurate co-relation of TC with IRI, if required.	Functional verification	
	2.1.15	TC and IRI shall be made available at the MC in near real time.	Functional verification	
	2.1.16	The system shall be able to support defined targets, based on interception criteria, for LEAs. For each LEA minimum targets assignment tentatively 5000, based on interception criteria, shall be possible at each site. The requirement of the supported targets shall be defined by Tendering Authority.	Functional verification (Refer Annex. I GR IPLC)	
	2.1.17	It shall be possible to simultaneously intercept a single target, based on interception criteria, by at least 12 LEAs. In such cases, each access shall be kept separate and distinct to ensure the privacy to each Law Enforcement Agency. The requirement of the minimum LEAs shall be defined by Tendering Authority.	Functional verification (Refer Annex. I GR IPLC)	
	2.1.18	Cross LEA keyword indexing should not be allowed i.e., querying on any given keyword should be allowed from the concerned LEAs targets in the database.	Functional verification	
	2.1.19	It shall be possible to define a new target type where an interception criterion is keyword(s).	Functional verification	
	2.1.20	IPLC-LIS shall support at least 500 concurrent keyword targets. The requirement of the minimum concurrent keyword targets shall be defined by Tendering Authority.	Functional verification/ Declaration (Refer Annex. I GR IPLC)	
	2.1.21	The interception-by-keywords shall support email and/or SMS filtering wherein keywords can be case insensitive and intercepted email and or SMS is fully captured. (Not clear appears ambiguous)	Functional verification	
	2.1.22	IPLC-LIS shall support Unicode texts and ASCII.	Functional verification	
	2.1.23	**Probe Buffer Capacity:** Probe should have sufficient buffer	Functional	

		storage to deal with interruption of link to Traffic aggregator; buffer storage capacity required to cater to temporary storage for atleast 2 days. Adequate temporary storage capacity may be defined so that no intercepted data is lost during link failure The requirement shall be defined by Tendering Authority within the IPLC/ISP.-----	verification (Refer Annex. I GR IPLC)	
2.2		Traffic Aggregator (TA)	Information	
	2.2.1	It shall receive the intercepted traffic from the probe(s) and send this IPLC traffic data to IPLC-LIM and to LEA who has requested the same in near real time in a secure manner over MPLS/ Internet network.	Functional verification	
	2.2.2	It shall be able to collect intercepted traffic from at least 8 Probes intercepting traffic using STM-256 interfaces. The actual requirement of capacity of TA for minimum intercepted traffic shall be defined by Tendering Authority. It shall support the filtering according to the Interception criteria as mentioned in clause 2.1.9.	Functional verification (Refer Annex. I GR IPLC)	
	2.2.3	It shall be able to detect duplicate packets that can come from different probes in the network, and eliminate them, so only a single copy is sent to the IPLC-LIM.	Functional verification	
	2.2.4	It shall be possible to configure the target, based on interception criteria, on traffic aggregator from Central as well as remote monitoring site(s) so that interception criteria can be further set on Probe.	Functional verification	
	2.2.5	It shall store the complete email/ chat/SMS in its memory for the purpose of spotting a keyword. In case the keyword is spotted, the whole email/ chat/SMS content (TC and IRI) shall be sent to central monitoring site otherwise the same may be deleted from memory and new mail/ chat/SMS session is taken for keyword spotting.	Functional verification	
	2.2.6	It shall be able to buffer intercepted traffic in case of failure of link to IPLC-LIM. It shall have the storage of data for at least 15 days. However the duration to be defined by Tendering Authority.	Functional verification Refer Annex. I GR IPLC	

	2.2.7	It shall be possible to store the information in separate files on the basis of target and IPLC-LIM.	Functional verification	
	2.2.8	Interface between IPLC-LIM and TA shall support file transfer standards like FTP (File Transfer Protocol) so that traffic aggregators from different vendors are able to work with central IPLC-LIM.	Functional verification	
	2.2.9	All communication between traffic aggregator and IPLC-LIM shall be encrypted/ secured using SSL (Secure Socket Layer), IP Sec (IP Security Protocols) or PKI (Public Key Infrastructure) over MPLS/Internet network.	Functional verification	
	2.2.10	Single TA shall be able to connect and transfer data to at least 12(Twelve) IPLC LIM simultaneously. TA shall communicate directly to the Analysis Servers or a Storage application server or Storage application running on the Analysis server.	Functional verification	
	2.2.11	It shall generate an alarm message in case of disconnection of link with the Probe. Alarm for such incidence shall be raised on maintenance terminal/ alarm panel of TA.	Functional verification	
	2.2.12	TA shall ensure during delivery that the intercepted data is delivered only to the proper LEAs while providing no visibility to additional LEAs that maybe targeting the same user. Thus, only the authorised LEA receives the intercepted data.	Functional verification	
	2.2.13	The system shall be capable to deliver the captured information to multiple LEAs, while keeping anonymity between the LEAs.	Functional verification	
	2.2.14	The system shall transform and transmit the TC and IRI to the proper LEA in the appropriate format.	Functional verification	
	2.2.15	The system shall support the following output and delivery formats:	Functional verification	

<table>
<tr><td></td><td></td><td>
<table>
<tr><th>Data Type</th><th>Output Format</th><th>Delivery Format</th></tr>
<tr><td rowspan="5">Traffic Content</td><td>Packet Capture (PCap)</td><td>File Transfer Protocol (FTP) / Secure FTP</td></tr>
<tr><td>J-STD-025B (ASN.1)</td><td>J-STD-025B (Data Stream)</td></tr>
<tr><td>Packet Cable</td><td rowspan="3">Custom</td></tr>
<tr><td>ETSI</td></tr>
<tr><td>Custom</td></tr>
<tr><td rowspan="9">Interception Related Information</td><td>XML</td><td>File Transfer Protocol (FTP) / Secure FTP</td></tr>
<tr><td>compact XML</td><td>Relational Database loader</td></tr>
<tr><td>J-STD-025B (ASN.1)</td><td>J-STD-025B (Data Stream)</td></tr>
<tr><td>IPDR (Format shall be in CSV / XML.)--</td><td rowspan="7">CSV/ XML/ JSON / ETSI</td></tr>
<tr><td></td></tr>
<tr><td>Flat file</td></tr>
<tr><td>annotated flat file</td></tr>
<tr><td>Packet Cable</td></tr>
<tr><td>ETSI</td></tr>
<tr><td>Custom</td></tr>
</table>
</td><td></td><td></td></tr>
<tr><td></td><td>2.2.16</td><td>The delivery mechanism shall be provided the ability to accept packets from multiple probes and an intermediate level of processing that re-orders packets from multiple locations into a full duplex stream.</td><td>Functional verification</td><td></td></tr>
<tr><td></td><td>2.2.17</td><td>The system shall enable listening to voice calls in near real time as well as off-line. Near real time function shall not necessitate additional traffic links to the LEA monitoring facility.</td><td>Functional verification</td><td></td></tr>
<tr><td></td><td>2.2.18</td><td>The near real time voice functionality shall be IP based so that LEA station can be easily mobilised. LEA workstation client must be web based.</td><td>Functional verification</td><td></td></tr>
<tr><td></td><td>2.2.19</td><td>Assignment of targets belonging to Data and TDM networks and target status view shall be possible from a single client.</td><td>Functional verification</td><td></td></tr>
<tr><td></td><td>2.2.20</td><td>IRI format: fields and format of IRI should be defined clearly like Target Identity, LIID, Time stamp of session initation, duration of session, IP address/Port, MAC ID, etc.</td><td>Functional verification</td><td></td></tr>
<tr><td>2.3</td><td></td><td>Diagnostic Facilities:</td><td>Declaration</td><td></td></tr>
<tr><td></td><td>2.3.1</td><td>The diagnostic capability of the system shall be such as to minimise the human efforts required.</td><td>Functional verification</td><td></td></tr>
<tr><td></td><td>2.3.2</td><td>Any malfunction in the system shall initiate a fault</td><td>Functional</td><td></td></tr>
</table>

		message and/or a visible maintenance procedure for location of the faulty unit or for detailed procedures on further action to be taken for rectification of the fault conditions. The classification of alarms in the system may be indicated.	verification	
	2.3.3	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 indications to a centralized place.	Functional verification	
2.4		**Power Supply:**	Declaration	
		The IPLC-LIS equipments shall work with -48 V DC (with the operating range as - 40 V to -60 V DC) or with AC supply (230 V AC +10%, -15% at 50 2 Hz frequency). The requirement of type of power supply and input range variation shall be defined in tendering requirements. The requirement of UPS with a backup time of 50% over dimensioning may also be included in the tendering requirements.	Functional verification	

	Technical Requirements of IPLC Traffic Lawful Interception Monitoring System (IPLC LIM)			
3.0		**Introduction:**	Information	
	3.0.1	IPLC-LIM is a functional unit, which shall be used for monitoring, storing and postprocessing of IPLC traffic. It shall have servers along with storage infrastructure for storing and post processing of the intercepted IPLC data, operation and maintenance consoles for the components of LIM system.	Declaration	
	3.0.2	It shall be possible to assign interception criteria and/or targets from any of the remote site and central monitoring site for IPLC traffic. The target configuration shall be done from the IPLC-LIM centrally on receipt of the request for interception from the LEAs.	Functional verification	
3.1		**Technical Requirements:**	Information	
	3.1.1	The IPLC–LIM shall consist of the following components:	Functional verification	
	3.1.1 (i)	Analysis Servers	Functional verification	
	3.1.1 (ii)	LAN Switches	Functional verification	
	3.1.1 (iii)	Firewall	Functional verification	
	3.1.1 (iv)	Intrusion Detection System (IDS)	Functional verification	
	3.1.1 (v)	Storage infrastructure	Functional verification	
	3.1.1 (vi)	Antivirus software	Functional verification	
	3.1.1 (vii)	Policy control and Element Management System (EMS)	Functional verification	
	3.1.1 (viii)	Database/Storage Server	Functional verification	

		The architecture of the IPLC-LIM is indicated in figure 2.	Information	
	3.1.2	The System shall be of high performance, high availability, scalable and centrally manageable. The system shall provide the support of integration of EMS with Network Management System.	Functional verification	
	3.1.3	The System shall provide a complete view into overall system and/or component health, as well as link status of the connections between components, which may be widely dispersed geographically.	Functional verification	
	3.1.4	The System shall provide control over the operational performance of all system components and it shall facilitate administrative tasks, such as:	Functional verification	
	3.1.4 (i)	License and access rights management	Functional verification	
	3.1.4 (ii)	Diagnostics and health monitoring	Functional verification	
	3.1.5	It shall communicate with the Traffic Aggregator(s) and consists of various servers, which are required for processing, and storage of the data sent by the IPLC-LIS.	Functional verification	
	3.1.6	It shall communicate with the IPLC-LIS in a secure manner and shall exchange data in near real-time.	Functional verification	
	3.1.7	The system shall support the data delivery formats and the interface requirements towards IPLC-LIS as defined in Chapter 2 under clause 2.2.	Functional verification	
	3.1.8	It shall be a fully protected, secure infrastructure deploying the state-of-art technology equipments. It shall deploy Firewall, IDS (Intrusion Detection System), Anti-Virus etc.	Functional verification	
	3.1.9	The following shall be supported in the IPLC-LIM:	Functional verification	
	3.1.9 (i)	Define and manage system users and targets/ group of targets.	Functional verification	
	3.1.9 (ii)	Start and stop of monitoring of target either automatically	Functional	

		or manually.	verification	
	3.1.9 (iii)	Assign targets to operators/ group of operators, depending on privileges, for monitoring at the terminal for optimal division of workload.	Functional verification	
	3.1.9 (iv)	Generate reports about system definitions and user activities, and maintain various system parameters.	Functional verification	
	3.1.9 (v)	Define the archiving framework for targets or grouping of targets.	Functional verification	
	3.1.9 (vi)	Manage all archiving devices within the system to ensure all required media are available and operational.	Functional verification	
	3.1.9 (vii)	Create, modify and delete targets or group of targets.	Functional verification	
	3.1.9 (viii)	Create and manage target's monitoring start and end date/time.	Functional verification	
	3.1.9 (ix)	Generate target related reports.	Functional verification	
	3.1.9 (x)	Generate reports for VoIP traffic based on calling & called numbers, volume, duration, origination & destination Country (Domestic and International) and protocol.	Functional verification	
	3.1.10	It shall have Monitoring/analysis server(s), which shall receive the intercepted traffic from the traffic aggregator(s) and reconstruct the packets into the original files (e.g. HTML, e-mail or SMS etc.).	Functional verification	
	3.1.11	It shall have Database Manager for managing the system database(s).	Functional verification	
	3.1.12	Each Monitoring/ Analysis Servers shall have file Logger, which shall store the intercepted traffic for short-term use. The storage shall be capable of storing at least data of fifteen days for each Law Enforcement Agency. The actual requirement of storage capacity shall be defined in tendering requirements (Refer Annex. I of this document).	Functional verification	
	3.1.13	It shall have offline storage to store the intercepted traffic and information added by users for long-term period on	Functional verification	

		removable media.		
	3.1.14	It shall be possible to protect stored data using suitable mechanism like hash functions etc.	Functional verification	
	3.1.15	It shall have Administrator workstation, which shall provide the control and administrator user interface. Workstation specification needs to be defined.	Functional verification	
	3.1.16	The LEAs shall be allowed to connect to the IPLC-LIM in a secure manner through the LEAs workstation so that they can get logged in to the Analysis Server and engage in Monitoring in near real time or can get the post processed Intercepted data.	Functional verification	
	3.1.17	The Analysis server(s) shall be capable of near real-time analysis of the incoming traffic.	Functional verification	
	3.1.18	It shall possible to examine the content of e-mail attachments and SMSs etc.	Functional verification	
	3.1.19	It shall be possible to do find/search on the intercepted data.	Functional verification	
	3.1.20	**Storage:** The Storage infrastructure to be deployed as part of the IPLC-LIM shall be as per latest TEC standard on DSI available on TEC website (https://tec.gov.in/standards-specifications)and shall consist of the following components:	Functional verification (Refer TEC Website)	
	3.1.20 (i)	Mid-Tier Storage: This shall be configured using the sufficient capacity of . NVMe enabled SSD Drive. The actual requirement of storage capacity for duration shall be defined in tendering requirements (Refer Annex. I of this document	Functional verification (Refer Annex. I GR IPLC)	
	3.1.20 (ii)	Online Archival Storage: This shall contain the raw/processed data intercepted by the probes and sent by the aggregators to the Mid tier storage and is more than one month old. The Online archival storage shall have the capacity atleast for duration shall be defined in tendering requirements (Refer Annex. I of this document). The archival storage system shall be connected to the LAN	Functional verification (Refer Annex. I GR IPLC)	

		Switch at IPLC-LIM over atleast 2 + 2 GigE electrical interface. The GigE interfaces shall be in two different modules and slots.		
	3.1.20 (iii)	Tape/Disk Library: NAS System: It shall have a capacity for a duration of data storage to be specified Tendering Authority (Refer Annex. I of this document).	Functional verification (Refer Annex. I GR IPLC)	
	3.1.20 (iv)	Storage Management: It shall consist of the Element Management System (EMS) or Storage Resources Management (SRM) and Hierarchical Storage Management System (HSM).	Functional verification	
	3.1.20 (v)	Fibre Channel Switch: Two Fibre channel Switches with each having atleast 16 FC ports or 1.5 times the Number of servers whichever is greater shall be deployed for implementing 'No Single Point of Failure (NSPOF)' Storage Architecture.	Functional verification	
	3.1.20.1	Sufficient capacity as indicated above for the purpose of storage and playing back for the various forms of traffic i.e. voice, fax and data including SMS, shall be provided.	Functional verification	
	3.1.20.2	The information may be stored according to different categories. For example, information that originates from different targets will be stored on different media.	Functional verification	
	3.1.20.3	It shall be possible to retrieve and present the IPLC intercepted traffic targetwise to an operator at a monitoring position, whenever requested through manmachine commands or GUIs from the SRM/HSM.	Functional verification	
	3.1.20.4	All Servers as part of the IPLC-LIM shall be managed through Enterprise Management System (EMS) which shall have to be supplied. All hardware 19 TEC Standard No. 49020:2025 components shall be rack mounted in server vendor's OEM rack. The number of racks shall be minimized for optimized floor space utilization.	Functional verification	
	3.1.20.5	Servers to be deployed at IPLC-LIM for applications i.e. Analysis Server, Storage server, EMS etc shall have	Functional verification	

		following peripherals/interfaces/HDD in addition to CPU, RAM and clustering requirements as indicated in schedule of requirements:		
	3.1.20.6	Servers shall use 64 bit CPUs of latest processor in the family and 3.0GHzor higher clock speed available from the bidder at the time of submission of bid. Exact requirement shall be defined by Tendering Authority (Refer Annex. I of this document).	Functional verification (Refer Annex. I GR IPLC)	
	3.1.20.7	The requirement of hardware sizing for servers, storage, appliances, management stations and consoles etc. shall be defined by Tendering Authority (Refer Annex. I of this document).	Functional verification (Refer Annex. I GR IPLC)	
3.2		**Power Supply:**	Declaration	
		The IPLC-LIM equipments shall work with AC supply 230 V AC +10%, -15% at 50+/- 2Hz frequency.	Functional verification	
	Operational and Management Requirements of IPLC Traffic Lawful Interception and Monitoring System (IPLC-LIMS)			
4.1		**Man Machine Communication:**	Information	
	4.1.1	The IPLC-LIMS shall be manageable using a user-friendly GUI (Graphical- User Interface). It shall be capable of performing all functions related to administration, management, supervision and maintenance of all kinds.	Functional verification	
	4.1.2	The operation and maintenance shall be supported by a set of user- friendly man machine commands. Man-machine language shall use English based commands and responses.	Functional verification	
	4.1.3	Calendar management for operator commands shall be available (It shall be possible to execute any command at any time by attaching a time tag to command and it shall be executed when the real time matches the time tag).	Functional verification	
	4.1.4	Adequate number of man-machine interface and input/ output devices shall be provided to facilitate operation and management. Minimum 12 number of monitoring	Functional verification (Refer Annex. I	

		positions with associated hardware and software shall be supported as per the user requirements. The actual requirement shall be defined in tendering requirements (Refer Annex. I of this document).	GR IPLC)	
	4.1.5	Suitable safeguards shall be provided in the man-machine communication programs to bar unauthorized persons from making any changes in the stored data contents.	Functional verification	
	4.1.6	The system shall protect users' access using a password with atleast two level categories like User/Super-user etc. The user shall able to monitor the targets defined for this user under category/authorisation etc.	Functional verification	
	4.1.7	The password shall be encrypted, so that it is impossible to retrieve it by sniffing to the system's LAN.	Functional verification	
	4.1.8	The system administrator shall be able to use various password policies like	Functional verification	
	4.1.8 (i)	forcing the users to modify the password on first login	Functional verification	
	4.1.8 (ii)	defining expiration-period for passwords	Functional verification	
	4.1.8 (iii)	defining required password complexity (combination of letters and numbers and minimum length)	Functional verification	
	4.1.8 (iv)	blocking access after a number of unsuccessful attempts.	Functional verification	
	4.1.9	The system shall provide audit trail for all user actions (e.g. defining a target, modifying a target, deleting a target, defining a user, modifying intercepted object's transcription). The system shall provide query tools for searching for specific audit events.	Functional verification	
	4.1.10	Access to system operations shall be controlled by at least two levels. The man machine language shall have facility for restricting the use of certain commands of procedures to certain staff/ terminals.	Functional verification	
	4.1.11	It shall be possible to store a log of commands given on admin/ user workstations and their responses in a read-only file in the system disk, which can be retrieved	Functional verification	

		whenever required by using man-machine commands. Alarm must appear in case of disk capacity utilization beyond pre defined limit.		
	4.1.12	The normal operation of the system shall not be affected while undertaking hardware expansion or enhancement of features.	Functional verification	
	4.1.13	The GUI/MMI shall provide the user with the ability to see the On-line activity, see the Off-line events, and do a synopsis of the traffic in a single screen.	Functional verification	
	4.1.14	When viewing web pages that were captured the view shall show the page as the target saw it, including handling of Java scripts, ActiveX elements, etc.	Functional verification	
	4.1.15	The system backup feature shall be provided on offline storages like CD/ DVD ROM, tape, etc.	Functional verification	
	4.1.16	Same LEA terminal shall be capable for monitoring the voice/data of IP and basic nature and mobile services. It may with the different client for these applications.	Functional verification	
4.2		**System Supervision**	Information	
	4.2.1	Provision made for continuous testing of the system to allow both system qualities check and fault indication as a fault arises.	Functional verification	
	4.2.2	The system shall provide for printouts and visual/audible alarms to assist in efficient administration.	Functional verification	
	4.2.3	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.	Functional verification	
	4.2.4	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.	Functional verification	
	4.2.5	Visual display of the different Probes and the control arrangement of the traffic aggregator shall be provided.	Functional verification	

4.3		**Diagnostic Facilities**	Information	
	4.3.1	The diagnostic capability of the system shall be such as to minimise the human efforts required.	Functional verification	
	4.3.2	Any malfunction in the system shall initiate a fault message and/or a visible maintenance procedure for location of the faulty unit or for detailed procedures on further action to be taken for rectification of the fault conditions. The classification of alarms in the system may be indicated.	Functional verification	
	4.3.3	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 indications to a centralized place.	Functional verification	
	4.3.4	The system shall have the capability to monitor its own performance and shall detect, analyse, locate and report faults.	Functional verification	
	4.3.5	**Target Provisioning through CMS**	Information	
	4.3.5 (i)	There should be an access class created in LIS/LIM exclusively for CMS based e provisioning of targets.	Functional verification	
	4.3.5 (ii)	No activity, targets provisioned, logs, etc pertaining to CMS shall be visible/retrievable to any other user/Administrator/O&M user in LIS/LIM.	Functional verification	
	4.3.6	**Remote Access (RA) restriction**	Information	
		Remote Access (RA) to LIS/LIM equipment from abroad is strictly prohibited. The remote access within india should be done only through secure/encrypted internal Data Links of the service provider.	Functional verification	
	4.3.7	**Defective Media/HDDs**	Information	
		The defective HDDs and other removable media should be destructed and should not send to OEM/Vendor for repair/replacement as it contains sensitive information.	Declaration	
	4.3.8	**Cyber Security**	Information	
		All best security practices should be adopted to secure	Functional	

		the LIS/LIM from getting compromised, as they are always the prime target of adversaries. There should be automatic alert system if there is any USB device insertions, malware detection, network property modifications etc.	verification	
5.0	**Engineering, Operational and Qualitative Requirements:**			
	5.0.1	**Engineering Requirements:** The system shall meet the following engineering requirements:	Declaration	
	5.0.1 (a)	The equipment shall be fully solid state and adopt state of the art technology.	Declaration	
	5.0.1 (b)	The equipment shall be compact, composite construction s: and light weight. The actual dimensions and weight of the equipment shall be furnished by the manufacturers.	Declaration	
	5.0.1 (c)	All connectors shall be reliable, low loss and standard type so as to ensure failure free operations over long operations.	Declaration	
	5.0.1 (d)	The equipment shall have adequate cooling arrangements, if required.	Declaration	
	5.0.1 (e)	Each sub-assembly shall be clearly marked with schematic reference to show its function, so that it is identifiable from the layout diagram in the handbook.	Declaration	
	5.0.1 (f)	Each terminal block and individual tags shall be numbered suitably with clear identification code.	Declaration	
	5.0.1 (g)	All controls, switches, indicators etc. shall be clearly marked to show their circuit diagrams and functions.	Declaration	
	5.0.2	**Operational Requirement (OR):** The system shall meet the following maintenance & operational requirements:	Declaration	
	5.0.2 (a)	The equipment shall be designed for continuous operation.	Declaration	
	5.0.2 (b)	The equipment shall be able to perform satisfactorily without any degradation at an altitude upto 3000 meters above mean sea level.	Declaration	
	5.0.2 (c)	Suitable visual indications shall be provided to indicate	Declaration	

		the healthy and unhealthy conditions.		
	5.0.2 (d)	The design of the equipment shall not allow plugging of a module in the wrong slot or upside down.	Declaration	
	5.0.2 (e)	The removal or addition of any cards shall not disrupt traffic on other cards.	Declaration	
	5.0.2 (f)	Special tools required for wiring shall be provided along with the equipment.	Declaration	
	5.0.2 (g)	In the event of a bug found in the software, the Manufacturer shall provide patches and firmware replacement if involved, free of cost. Compatibility of the existing hardware shall be maintained with future software/firmware.	Declaration	
	5.0.2 (h)	A power down condition shall not cause loss of connection configuration data storage.	Declaration	
	5.0.2 (i)	Live Insertion and hot swap of modules shall be possible to ensure maximum network availability and easy maintainability.	Declaration	
	5.0.2 (j)	IPLC-LIMS shall not have any single point of failure.	Declaration	
	5.0.2 (k)	OEM shall provide regular software / firmware updates along with security updates as and when available offline.	Declaration	
	5.0.3	**Qualitative Requirements (QR):** The system shall meet the following qualitative requirements:	Declaration	
	5.0.3.1	The manufacturer shall furnish the MTBF value. Minimum value of MTBF shall be specified by the purchaser. The calculations shall be based on the guidelines given in either QA document No. QM-115 {January 1997} "Reliability Methods and Predictions" or any other international standards.	Declaration	
	5.0.3.2	The equipment shall be manufactured in accordance with international quality management system ISO 9001:2015 or any other equivalent ISO certificate for which the manufacturer should be duly accredited. A quality plan describing the quality assurance system followed by the	Declaration	

		manufacturer would be required to be submitted.		
	5.0.3.3	The equipment shall conform to the requirements for Environment specified in TEC QA standards QM-333 {Issue- March, 2010}(TEC 14016:2010) "Standard for Environmental testing of Telecommunication Equipments" or any other equivalent international standard, for operation, transportation and storage. The applicable environmental category A or B to be decided by the purchaser based on the use case.	Declaration	
	5.0.4	**Electromagnetic Compatibility (EMC):**	Information	
		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 from accredited test lab shall be furnished from a test agency.	Declaration	
	5.0.4 (a)	**Conducted and radiated emission (applicable to telecom equipment):**	Information	
		Name of EMC Standard: "CISPR 32 (2015) with amendments - Limits and methods of measurement of radio disturbance characteristics of Information Technology Equipment".	Information	
		Limits:- i) To comply with Class B of CISPR 32 (2015) with amendments for indoor deployments and Class A of CISPR 32 (2015) with amendments with amendments for outdoor deployments.	Declaration	
	5.0.4 (b)	**Immunity to Electrostatic discharge:**	Information	
		Name of EMC Standard: IEC 61000-4-2 {2008) "Testing and measurement techniques of Electrostatic discharge immunity test".	Information	
		Limits:- i) Contact discharge level 2 {± 4 kV} or higher voltage;	Declaration	
		ii) Air discharge level 3 {± 8 kV} or higher voltage;	Declaration	

	5.0.4 (c)	**Immunity to radiated RF:**	Information	
		Name of EMC Standard: IEC 61000-4-3 (2010) "Testing and measurement techniques-Radiated RF Electromagnetic Field Immunity test".	Information	
		Limits:- **For Telecom Equipment and 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.	Declaration	
	5.0.4 (d)	**Immunity to fast transients (burst):**	Information	
		Name of EMC Standard: IEC 61000-4-4 {2012) "Testing and measurement techniques of electrical fast transients/burst immunity test".	Information	
		Limits:- Test Level 2 i.e. a) 1 kV for AC/DC power lines;	Declaration	
		b) 0. 5 kV for signal / control / data / telecom lines;	Declaration	
	5.0.4 (e)	**Immunity to surges:**	Information	
		Name of EMC Standard: IEC 61000-4-5 (2014) “Testing & Measurement techniques for Surge immunity test".	Information	
		Limits:- i) For mains power input ports :	Declaration	
		(a) 2 kV peak open circuit voltage for line to ground coupling	Declaration	
		(b) 1 kV peak open circuit voltage for line to line coupling	Declaration	
		ii) For telecom ports :	Declaration	
		(a) 2kV peak open circuit voltage for line to ground	Declaration	
		(b) 2KV peak open circuit voltage for line to line coupling.	Declaration	
	5.0.4 (f)	**Immunity to conducted disturbance induced by Radio**	Information	

		frequency fields:		
		Name of EMC Standard: IEC 61000-4-6 (2013) with amendments) "Testing & measurement techniques- Immunity to conducted disturbances induced by radio-frequency fields".	Information	
		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.	Declaration	
	5.0.4 (g)	**Immunity to voltage dips & short interruptions (applicable to only ac mains power input ports, if any):**	Information	
		Name of EMC Standard: IEC 61000-4-11 (2004) "Testing & measurement techniques- voltage dips, short interruptions and voltage variations immunity tests".	Information	
		Limits:- i) A voltage dip corresponding to a reduction of the supply voltage of 30% for 500ms (i.e. 70 % supply voltage for 500 ms)	Declaration	
		ii) A voltage dip corresponding to a reduction of the supply voltage of 60% for 200ms; (i.e. 40% supply voltage for 200ms) and	Declaration	
		iii) A voltage interruption corresponding to a reduction of supply voltage of > 95% for 5s.	Declaration	
		iv) A voltage interruption corresponding to a reduction of supply voltage of >95% for 10s.	Declaration	
	5.0.4 (h)	**Immunity to voltage dips & short interruptions (applicable to only DC power input ports, if any):**	Information	
		Name of EMC Standard: IEC 61000-4-29:2000: Electromagnetic compatibility (EMC) - Part 4-29: Testing and measurement techniques - Voltage dips, short interruptions and voltage variations on d.c. input power port immunity tests.	Information	
		Limits:-	Declaration	

		i) Voltage Interruption with 0% of supply for 10ms. Applicable Performance Criteria shall be B.		
		ii) Voltage Interruption with 0% of supply for 30ms, 100ms, 300ms and 1000ms. Applicable Performance Criteria shall be C.	Declaration	
		iii) Voltage dip corresponding to 40% & 70% of supply for 10ms, 30 ms. Applicable Performance Criteria shall be B.	Declaration	
		iv) Voltage dip corresponding to 40% & 70% of supply for 100ms, 300 ms and 1000ms. Applicable Performance Criteria shall be C.	Declaration	
		v) Voltage variations corresponding to 80% and 120%of supply for 100 ms to10s as per Table 1c of IEC 61000-4-29. Applicable Performance Criteria shall be B.	Declaration	
		Note: - 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 (TEC 11016:2016) and the referenced base standards i.e. IEC and CISPR standards 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 (h) and TEC Standard TEC/SD/DD/EMC-221/05/OCT-16. The details of IEC/CISPR and their corresponding Euro Norms are as follows:	Declaration	
		Euro Norms are as follows:	Declaration	

		IEC/CISPR — Euro Norm CISPR 11 — EN 55011 CISPR 32 — EN55032 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 IEC 61000-4-29 — EN 61000-4-29		
	5.0.5	**Safety Requirements:**	Information	
		The equipment shall conform to relevant safety requirements as per IS/IEC 62368-1:2018 or Latest as prescribed under Table no. 1 of the TEC document 'SAFETY REQUIREMENTS OF TELECOMMUNICATION EQUIPMENT":TEC10009:2024.The manufacturer/supplier shall submit a certificate in respect of compliance to these requirements	Declaration	
	5.0.6	**Other Requirements:**	Information	
		a) The system hardware / software shall not pose any problem, due to changes in date and time caused by events such as changeover of millennium / century, leap year etc., in the normal functioning of the system.	Functional verification	
		b) Wherever, the standardized documents like ITU-T, IETF, QA, TEC etc. documents are referred, the latest issue and number with the amendments shall be applicable.	Functional verification	
		c) **Power Supply:** The equipment power supply requirements details are given in Chapter 1. In	Information	

		addition, it shall meet the following requirements:		
		i. The equipment shall be able to function over the range specified in the respective chapters, without any degradation in performance.	Declaration	
		ii. The equipment shall be protected in case of voltage variation beyond the range specified and also against input reverse polarity.	Declaration	
		iii. The derived DC voltages shall have protection against short circuit and overload.	Declaration	
		Documentation, Installation and Software Maintenance		
6.0		**Documentation :**	Information	
		This chapter describes the general requirements for documentation to be provided for IPLC-LIMS. All technical documents shall be in English language both in CD ROM and in hard copy.	Declaration	
		The documents shall comprise of:	Declaration	
		a) System description documents.	Declaration	
		b) Installation, Operation and Maintenance documents.	Declaration	
		c) Training documents.	Declaration	
		d) Repair manual.	Declaration	
	6.0.1	**System description documents:**	Information	
		The following system description documents shall be supplied along with the system:	Declaration	
		a) Over-all system specification and description of hardware and software.	Declaration	
		b) Equipment layout drawings.	Declaration	
		c) Cabling and wiring diagrams.	Declaration	
		d) Schematic drawings of all circuits in the system with timing diagrams wherever necessary.	Declaration	
		e) Detailed specification and description of all Input / Output devices.	Declaration	
		f) Adjustment procedures, if there are any field	Declaration	

		adjustable units.		
		g) Spare parts catalogue – including information on individual component values, tolerances, etc. enabling procurement from alternative sources.	Declaration	
		h) Detailed description of software describing the principles, functions, and interactions with hardware, structure of the program and data.	Declaration	
		i) Detailed description of each individual software package indicating its functions and its linkage with the other packages, hardware, and data.	Declaration	
		j) Program and data listings.	Declaration	
		k) Graphical description of the system. In addition to the narrative description a functional description of the system using the functional Specification.	Declaration	
	6.0.2	**System operation documents:**	Information	
		The following system operation documents shall be available:	Declaration	
		a) Installation manuals and testing procedures.	Declaration	
		b) Precautions for installation, operations and maintenance.	Declaration	
		c) Operating and Maintenance manual of the system.	Declaration	
		d) Safety measures to be observed in handling the equipment.	Declaration	
		e) Man-machine language manual.	Declaration	
		f) Fault location and trouble shooting instructions including fault dictionary.	Declaration	
		g) Test jigs and fixtures required and procedures for routine maintenance, preventive maintenance and unit / card / sub-assembly replacement.	Declaration	
		h) Emergency action procedures and alarm dictionary.	Declaration	
	6.0.3	**Training Documents:**	Information	
		a) Training manuals and documents necessary for	Declaration	

		organizing training in installation, operation and maintenance and repair of the system shall be made available.		
		b) Any provisional document, if supplied, shall be clearly indicated. The updates of all provisional documents shall be provided immediately following the issue of such updates.	Declaration	
		c) The structure and scope of each document shall be clearly described.	Declaration	
		d) The documents shall be well structured with detailed cross-referencing and indexing enabling easy identification of necessary information.	Declaration	
		e) All diagrams, illustrations and tables shall be consistent with the relevant text.	Declaration	
	6.0.4	**Repair Manual:**	Information	
		a) List of replaceable parts used.	Declaration	
		b) Detailed ordering information for all the replaceable parts.	Declaration	
		c) Procedure for trouble shooting and sub-assembly replacement.	Declaration	
		d) Test fixtures and accessories for repair.	Declaration	
		e) Systematic trouble shooting charts (fault tree) for all the probable faults with their remedial actions.	Declaration	
	6.0.5	**Installation:**	Information	
		a) All necessary interfaces, connectors, connecting cables and accessories required for satisfactory installation and convenient operations shall be supplied. Type of connectors, adopters to be used shall be in conformity with the interfaces defined in this GR.	Declaration	
		b) It shall be ensured that all testers, tools and support required for carrying out the stage by stage testing of the equipment before final commissioning of the	Declaration	

		network shall be supplied along with the equipment.		
		c) All installation materials, consumables and spare parts to be supplied.	Declaration	
		d) All literature and instructions required for installation of the equipment, testing and bringing it to service shall be made available in English language.	Declaration	
		e) For the installations to be carried out by the supplier, the time frames shall be furnished by the supplier including the important milestones of the installation process well before commencing the installations.	Declaration	
		f) The equipment shall have:	Declaration	
		i. Proper earthing arrangement.	Declaration	
		ii. Protection against short circuit / open circuit.	Declaration	
		iii. Protection against accidental operations for all switches / controls provided in the front panel.	Declaration	
		iv. Protection against entry of dust, insects and lizards.	Declaration	
	ANNEX-I			
		Tendering/Ordering information: The following information shall be mentioned in tendering document:	Information	
		A. For IPLC-LIS :	Information	
	1.1.4	The requirement of bandwidth for IPLC-LIMS i.e. for connectivity between IPLC-LIS and IPLC-LIM.	Information	
	2.0 (a)	The figure for the insertion loss for probes.	Information	
	2.1.2	The type/s and number of Probe/s.	Information	
	2.1.4	Type and numbers of interfaces intercepting the IPLC traffic.	Information	
	2.1.5	Type of different protocols (latest versions) allowed to be aggregated to a router or directly supported by the IP-Probe.	Information	
	2.1.12 & 2.1.23	The requirement of the Probe data buffering duration.	Information	
	2.1.16	The requirement of the supported and minimum targets.	Information	

	2.1.17	The requirement of the minimum LEAs.	Information	
	2.1.1.20	The requirement of the minimum concurrent keyword targets.	Information	
	2.2.2	The requirement of capacity of TA for minimum total intercepted traffic.	Information	
	2.2.6	The duration of the storage of data for buffer intercepted traffic in case of failure of link to IPLC-LIM.	Information	
	2.4	The requirement of type of power supply with input range and UPS with a backup time of 50% over-dimensioning.	Information	
		B. For IPLC-LIM :	Information	
	1.1.4	The requirement of bandwidth for IPLC-LIMS i.e. for connectivity between IPLC-LIS and IPLC-LIM.	Information	
	1.1.6	The scalability of IPLC-LIMS equipment.	Information	
	3.1.12	The actual requirement of storage capacity for storing at least data of seven days for each Law Enforcement Agency.	Information	
	3.1.20 (i)	The actual requirement of storage capacity for Mid-Tier Storage.	Information	
	3.1.20 (ii)	The Online archival storage the capacity and minimum duration.	Information	
	3.1.20 (iii)	Tape/Disk Library/NAS storage capacity.	Information	
	3.1.20.6	The requirement of CPU, Processor for servers.	Information	
	3.1.20.7	The requirement of hardware sizing for servers, storage, appliances, management stations and consoles etc	Information	
	4.1.4	Adequate number of man-machine interface and input/ output devices.	Information	
		ANNEX-II		
		Items to be mentioned on Type Approval Certificate:	Information	
		a) Software version of **LIMS**.	Information	
		b) Type of interfaces supported (Clause 2.1.4).	Information	
		c) Numbers of Authorized Law Enforcement Agencies (LEAs) supported.	Information	

I. TEST SETUP & PROCEDURES:

1. Test No.	
2. Test Details	*Name and Other relevant details*
3. Test Instruments Required	1. <Name> 2.
4. Test Setup	
5. Test Procedure	*Testing Steps may be written here…..* 1. …….. 2. …….. 3. ……..
6. Test Limits	(*if any*)
7. Expected Results	1. ……..<values>…… 2. ……..<values>…… 3.

Further Test Setup & Procedures may be added as per requirement

J. SUMMARY OF TEST RESULTS

TEC Standard No. _____

TEC Test Guide No. _____

Equipment name & Model No. _____

Clause No.	*Compliance* *(Compiled /Not Compiled /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'.***

Annexure

Comments on Revision of Test Guide Titled "International Private Leased Circuit (IPLC) Traffic Lawful Interception and Monitoring System (IPLC-TLMS)"

(Draft Test Guide Standard No. TEC 49021:2025)

Name of

Manufacturer/Stakeholder:

Organization:

Contact details:

Clause No.	Clause	Comments	Other Remarks, if any

Note: The Comments on the revision of Test Guide titled "International Private Leased Circuit (IPLC) Traffic Lawful Interception and Monitoring System (IPLC-TLMS)" may be provided in the above format vide Email to adic1.tec@gov.in, adit2.tec-dot@gov.in, dirit2.tec-dot@gov.in