TENDER DOCUMENT

Tender for Supply, installation,Testing and Commissioning of Security Testing tools at TEC New Delhi

2-1/2021-MM/TEC Dated 06.10.2021

ISO 9001:2015

Government of India
Ministry of Communications
Department of Telecommunications
TELECOMMUNICATION ENGINEERING CENTRE,
Khurshid Lal Bhawan, Janpath, New Delhi - 110001

(Visit at www.eprocure.gov.in or www.tec.gov.in)

Stamp and signature of bidder

TABLE OF CONTENT

SECTION - I
NOTICE INVITING TENDER

Govt. of India
Ministry of Communications
Department of Telecommunications
Telecommunication Engineering Centre
Khurshid Lal Bhawan, Janpath,
New Delhi – 110001

Tender No. 2-1/2021-MM/TEC
Dated 06.10.2021

Tenders are invited by Sr. DDG, Telecom Engineering Centre (TEC), on behalf of President of India, only from Original equipment manufacturers or their authorized suppliers for supply of various item(s)/tool(s) stated in table 2 below for setting up of Security Test lab at TEC New Delhi in accordance with table 1 below.

Table -1:

Approximate cost of Tender	Rs.14.85Crores
Earnest Money Deposit	(As specified in NIT)
Date/Time of Publishing of e-Tender	06.10.2021
Document Download Start Date/Time	1500 Hrs of 06.10.2021
Document Download End Date/Time	1500 Hrs of 10.12.2021
Clarification Start Date/Time	1500 Hrs of 06.10.2021
Date & Time of Pre Bid Conference	1100 Hrs of 18.10.2021
Clarification End Date/Time	1700 Hrs of 20.10.2021
Bid Submission Start Date/Time	1500 Hrs of 19.11.2021
Bid Submission End Date/Time	1500 Hrs of 10.12.2021
Date/Time of opening of Techno-commercial Bid	1500 Hrs of 13.12.2021

Table -2:

EMD and turnover requirement against each item are given below. Bidders are free to quote for one or more items. In case the bidder quotes more than one item, the EMD and turnover requirement shall be the sum of individual EMDs and turnovers mentioned against respective items in the table given below.

Sr. No.	**Item**	**Quantity**	**EMD (In ₹)**	**Turnover (In ₹)**
1	Vulnerability Assessment tool (CVE Complied)	**1**	**55 Thousands**	**1.10 Crores**

Stamp and signature of bidder

2	Vulnerability Assessment tool (CCS 7 related)	**1**	**30 Thousand**	**60 Lakhs**
3	Fuzzing tool (Ethernet Interface)	**1**	**20 Lakhs**	**32 Crores**
4	Static code Analysis and Dynamic Analysis Application Security Testing Tool)	**1**	**2 Lakhs**	**4 Crores**
5	Binary Analysis Tool	**1**	**1.4 lakhs**	**2.8 Crores**
6	Penetration Testing Tool	**1**	**80 Thousand**	**1.55 Crores**

The tender document is available on website http://eprocure.gov.in. The intending bidders may download the e-tender document from the above mentioned website. The interested bidders may submit the bids online at https://eprocure.gov.in in two bids systems {i.e. (i) Techno-commercial Bid and (ii) Financial Bid} in the prescribed proforma. Bids are to be submitted only online through the e-procurement portal https://eprocure.gov.in/eprocure/app. All the documents in support of bid are also to be scanned and uploaded along with the tender document. Bid sent by any other mode will not be accepted.

The bidder shall upload the e-bids and submit original 'Pre-Bid/Pre-Contract Integrity Pact', Indemnity Bond, Demand Drafts/Banker's Cheque/BG/FD i.r.o. EMD, drawn in any Scheduled Bank in Delhi, in favour of Accounts Officer (Cash) TEC, New Delhi, in Room No 257, Khurshid Lal Bhawan, TEC, before scheduled date & time. E-Bid submitted without EMD in the prescribed format will not be accepted.

ADG (MM)
TEC, New Delhi
AX No.: 011-23725144

Stamp and signature of bidder

SECTION - II
INSTRUCTIONS TO BIDDERS

1.0 DEFINITIONS:

a. "The Purchaser" means the Telecommunication Engineering Centre (TEC).
b. "The e-bidder" means a company or firm who participates in this tender and submits its e-bid. (hereafter e-bidder shall be referred as bidder)
c. "The Supplier/Contractor" means a company or firm supplying the item(s) and providing the services as per SOR, under the contract.
d. "The Goods" means all the equipment, measuring instruments, Computer Hardware/ Software and/ or other materials, which the Supplier is required to supply to the Purchaser under the contract.
e. "The Advance Purchase Order" means the intention of Purchaser to place the Purchase Order on the successful bidder.
f. "The Purchase Order" means the order placed by the Purchaser on the Supplier signed by the Purchaser including all attachments and appendices thereto and all documents incorporated by reference therein. The purchase order shall be deemed as "Contract" appearing in the document.
g. "The Contract Price" means the price payable to the Supplier under the purchase order for the full and proper performance of its contractual obligations.
h. "Contract Period" means the period starting from the placement of PO and ending with expiry of the SLA.
i. "Testing tool" shall mean software as well as the associated hardware.

1.1 **REGISTRATION AT E-PROCUREMENT PORTAL**:

For participating in bidding through the e-procurement portal, it is necessary for the bidders to be the registered users of the e-procurement portal; http://eprocure.gov.in. For Bidders guidance **Bidders Manual Kit** is available at http://eprocure.gov.in/eprocure/app.

2.0 ELIGIBLE BIDDERS:

2.1 **General**

2.1.1 The bidder for this tender shall be an OEM (Original Equipment Manufacturer) or its authorized supplier of the quoted item(s) as per SOR (Schedule of requirement) as mentioned in Section V B.

2.2 **Bidder Company Status:**

2.2.1 The bidder company shall be registered and incorporated in India under the Companies Act, 1956 or Companies Act, 2013. In case of firm, it shall be registered under the relevant law.

2.2.2 In case of authorized suppliers of respective OEM(s), the bidder shall ensure that there is appropriate teaming arrangement / MOU with the respective OEM for successful installation, acceptance testing, warranty, updation, upgradation, accreditation and SLA of testing tool(s) for which the bidder has quoted, for the entire period of contract. For this bidder must submit the MOU/OEM Authorization clearly indicating that the bidder is an authorized

supplier of the respective OEM(s) and respective OEM's commitment for successful installation, acceptance testing, warranty, updation, upgradation, accreditation and SLA of testing tool(s) for the entire period of contract.

2.3 **Technical Experience:**

2.3.1 For the supply of testing tools, the bidder or its partner OEM shall have capability and experience in development and implementation of test scripts for various quoted testing tools as per SOR to facilitate automated test processes. In support of the above, the bidder or its partner OEM shall submit the documentary proof for the supply of quoted item(s) to atleast three telecom operator/regulator/government/manufacturer/ independent entity during the past five years from the date of submission of bids. The bidder should also submit an undertaking that the supplied equipment are functioning satisfactorily.

Supporting documents having older software and hardware versions than the software and hardware versions quoted in the bid shall be acceptable for the compliance of clauses 2.3.1

2.3.2 In case the partner OEM of the bidder is an Indian subsidiary of a Foreign OEM, either Indian Subsidiary of OEM or its Parent Company shall jointly or individually meet the Technical Experience criteria mentioned at clause 2.3.1.

2.4 **Turnover:**

The bidder eligible to participate in the tender for supply of item(s) as per Schedule of Requirement (Section-V-B) (in case of Indian subsidiary of a foreign OEM, either Indian subsidiary or its parent company) shall have Annual audited financial turnover of at least the amount tabulated below, during each of the 3 consecutive financial years (FY 2017-18, 2018-19 & 2019-20). In case the turnover is in foreign currency, the SBI exchange rate as on the date of the actual opening of the bid shall be taken into account.

Sr. No.	**Item**	**Quantity**	**Turnover (in Rs.)**
1	Vulnerability Assessment tool (CVE Complied)	**1**	**1.10 Crores**
2	Vulnerability Assessment tool (CCS 7 related)	**1**	**60 Lakhs**
3	Fuzzing tool (Ethernet Interface)	**1**	**32 Crores**
4	Static code Analysis and Dynamic Analysis Application Security Testing Tool)	**1**	**4 Crores**
5	Binary Analysis Tool	**1**	**2.8 Crores**
6	Penetration Testing Tool	**1**	**1.55 Crores**

In case the bidder quotes for more than one item, the turnover shall be the sum of individual turnovers mentioned against those items in the above table. Prior turnover for micro and small enterprises shall be relaxed subject to the fulfilment of conditions as stated in MSME policy circular no. 1(2)(1)/2016-MA dated 10.03.2016. However, for this relaxation, the bidder shall submit the relevant supporting document.

2.5 **Certification:**

The bidder who may participate in the supply of item(s) as per Schedule of Requirement (Section-V-B) or the respective partner OEM(s) shall have a valid (on the date of opening of tender) TL9000 or ISO 9001:2015 certification or latest version of TL or ISO certification.

3.0 COST OF BIDDING:

The bidder shall bear all costs associated with the preparation and submission of the bid. The Purchaser, will in no case, be responsible or liable for any costs, regardless of the conduct or outcome of the bidding process.

4.0 DOCUMENTS COMPRISING THE e-TENDER:

4.1 The goods required, bidding procedures and contract terms are prescribed in the Bid Document. The Bid Document includes:

a. Notice inviting tender
b. Instructions to bidders
c. General (commercial) conditions of contract
d. Special conditions of contract
e. Technical specifications & schedule of requirement
f. Pre-bid/pre-contract integrity pact
g. Indemnity Bond
h. Profile of bidder
i. EMD BG Form
j. No near Relative Declaration/Certificate
k. Performance security bond form
l. Bid Form
m. Technical Proforma
n. List of Protocols and File formats
o. No Blacklisting Declaration/Certificate

4.2 Price Schedule shall be filled separately in Financial Bid of the tender, as per the procedure given in Bidders Manual Kit.

4.3 The bidder is expected to examine all instructions, forms, terms and specifications in the e-tender document. Failure to furnish all information as per the e- tender document or submission of e-bid not as per the requirement of e-tender document in every respect will be at the bidder's risk and may result in rejection of the said e-bid.

5.0 CLARIFICATIONS/AMENDMENTS OF e-TENDER DOCUMENT:

5.1 A prospective bidder requiring any clarification on the tender document shall upload its queries on e-procurement portal, prior to **1700 HRS OF 20.10.2021.**

5.2 Purchaser shall upload the response to such queries, which are received in due time, generally by 21 days prior to the date of opening of the bids.

5.3 At any time, prior to the date of submission of bids, Purchaser may, for any reasons whether at its own initiative or in response to a clarification sought by a prospective bidder, modify the e-tender document by amendments.

5.4 The amendments/clarifications, if any, which are uploaded on the portal www.eprocure.gov.in, shall form an integral part of the tender document, and shall be binding on all bidders.

5.5 It shall be the sole responsibility of the prospective bidder to check the web site http//eprocure.gov.in from time to time for any amendment in the e-tender documents. In case of failure to get the amendments, if any the department shall not be responsible for it. Interested bidders are required to keep abreast of latest corrigendum (s) issued by Purchaser till the date of submission of bid.

6.0 PRE-BID CONFERENCE:

6.1 A Pre-bid conference shall be held at 1100 Hrs of 18.10.2021 in the MANAK, Ground floor, Telecom Engineering Centre, Khurshid Lal Bhawan, New Delhi. The queries already received shall, to the extent possible, be clarified in a Pre-bid Conference. The prospective bidders may attend the conference for clarifications on technical specifications, and other terms and conditions of the tender document. The queries, verbally raised during the Pre-Bid conference, must be uploaded in the portal by 1700 Hrs of 20.10.2021. Consolidated replies to the relevant uploaded queries, shall form part of the tender document, and shall be uploaded on the web-sites, generally by 21 days prior to the date of opening of the bids.

6.2 For interpretation of any condition of this tender document, the decision of purchaser shall be final and binding on the Prospective Bidder.

6.3 In order to afford prospective bidders a reasonable time to take the amendment into account in preparing their bids, the purchaser may, at its discretion, extend the deadline for the submission of bids suitably.

7.0 DOCUMENTS COMPRISING THE BID TO BE UPLOADED:

The bid prepared by the bidder shall comprise of:

(1) Techno-commercial bid, and

(2) Financial bid

7.1 All documents to be submitted under the bid must be uploaded in pdf format along with scanned copy of Demand Draft/Banker's Cheque/BG/FD for Earnest Money Deposit. However, original 'Pre-Bid/Pre-Contract Integrity Pact', Indemnity Bond, Demand Drafts/Banker's Cheque/BG/FD i.r.o. EMD shall be submitted in Room No 257, Khurshid Lal Bhawan, TEC upto the last date of submission of e-bids (1500 Hrs of 10.12.2021 The purchaser reserves

Stamp and signature of bidder

the right to seek actual documents for any uploaded documents during evaluation of the e-bid.

7.2 **The Techno-commercial e-bid for 2-1/2021-MM/TEC dated 06.10.2021 should contain**:

7.2.1 Documents required to meet the eligibility criteria: These documents are vital for evaluation and bidder must take utmost care while uploading these documents complete in all respects.

a Scanned copy of Demand Draft/Banker's Cheque/BG/FD from Scheduled Bank of India for the prescribed amount (As per table 2 of NIT) of earnest money deposit **along with the list of quoted item(s) for which EMD has been submitted.**

b Latest NSIC certificates and documents, if applicable

c Authorization letter for signing the bid document(s) in the form of Board Resolution/Power of Attorney or letter of authorization duly signed by all partners/proprietor on the letterhead of the firm/company, as applicable.

d Copy of Certificate of Registration of company/firm as per clause no. 2.2.1 of Section II.

e A copy of MOU between bidder and OEM(s) or OEM(s) Authorization letter (as per template draft in Annexure XI) as required in clause no. 2.2.2 of section II shall be provided, if the bidder is an authorized supplier of an OEM(s).

f Complete Audited financial report as a proof for annual turnover of preceding three financial years as mentioned in clause 2.4 of Section II, as applicable, or requisite certificate/document(s) as per MSME policy circular no. 1(2)(1)/2016-MA dated 10.03.2016, for relaxation of turnover.

g Copies of Purchase Order along with proof of supply as per Clause No.2.3.1/ of Section II. The bidder shall also submit an undertaking that the supplied tools are functioning satisfactorily.

h Copy of valid Certificate confirming TL9000 or ISO 9001:2015 certification or latest, as per clause 2.5 of Section II.

i Copy of the duly executed Pre-Bid/Pre-Contract Integrity Pact (Refer Clause 17.1 of Section II).

j Tender document (consisting of all Sections and Annexures, Subsequent Amendments/Clarifications if any), duly filled and signed by the authorised signatory with the stamp of the bidder.

7.2.2 Supporting documents: These documents as indicated below shall also be uploaded as part of the bid.

a List, giving full particulars of *software including licences* etc., necessary for the proper and continuous functioning of the offered tool(s) for the entire contract period, wherever applicable shall be submitted along with undertaking from the bidder that all the software including licenses as indicated above are being proposed to be supplied in the bid are of perpetual nature.

Stamp and signature of bidder

b List of Partners/directors of the bidder along with Partnership Deed or Article/Memorandum of Association, as applicable.

c For supply of any software, the bidder shall submit the Certificate of the OEM countersigned by Authorized Signatory of the bidder stating that all software supplied are authentic and legal copy is/are being supplied, wherever applicable.

d Duly filled and signed Profile of bidder as per Annexure III.

e Copy of PAN card/ GIR card and copy of GST registration Certificate of the organization.

f Duly filled Bid Form as per Annexure VII.

g No near relative Certificate/Declaration as per Annexure-V.

h Duly filled Technical Proforma as per Annexure VIII mentioning name of his OEM, brand name and model no along with software version of the products offered in this tender. Technical literature of the products along with clause by clause compliance of the technical requirements mentioned in Section V of the tender document should also be submitted as per clause 9.4, Section II in the form of Annexure XII.

i Copy of Indemnity Bond as per Annexure-II.

j No blacklisting declaration/certificate as per Annexure X.

7.3 **Price Schedule** for **tender no. 2-1/2021-MM/TEC dated 06.10.2021** shall be filled separately as given in Financial bid .Bidder shall submit the financial bid for individual item(s) as per SOR (Section V B)

7.4 The bidder is expected to examine all instructions, forms, terms & conditions and specifications in the Tender Document and amendments/ clarifications, if any, and submit the bid accordingly.

7.5 No tender shall be uploaded after 1500 Hrs of 10.12.2021. Only in case the last date of submission of bids is declared as Central Government holiday in Delhi, the original EMD will be accepted up to the next working day till the same time and the Techno-commercial Bid will be opened on the next working day at the scheduled time.

7.6 Tender document, as downloaded, must be submitted without making any additions, alternations. Bid containing unauthorized amended/modified Tender document is liable to be rejected.

7.7 The purchaser reserves the right to accept/reject any/all/part of the bids without assigning any reason.

7.8 Any bid unaccompanied by EMD in variance with the instructions herein, is liable to be rejected summarily.

7.9 The bid shall contain no interlineations, erasures or overwriting except as necessary to correct errors made by the bidder in which case such corrections shall be signed by the person or persons authorized for signing the bid.

7.10 In case any requisite document(s) is submitted with bid in any language other than Hindi or English, the duly signed copy of the translation of that document from any authorised translator shall also be submitted along with the bid document.

7.11 In case of power of Attorney for participation in tender and signing the document(s), on behalf of the Company/ Institution/Body corporate/Firm, same should be executed on the non-judicial stamp paper of appropriate value and as per prevailing guidelines in the respective state(s).

8.0 BID PRICES:

8.1 The prices should be quoted only in Indian Rupees as per Price Schedule only. No foreign exchange shall be made available by the purchaser. The Unit price after discount, if any and all other components need to be quoted individually.

8.2 The bidder must quote a definite price for quoted item(s) and its components.

8.3 For the item(s) not being quoted by the bidder, the column mentioned in price schedule for "Unit Rate (After discount, if any) in Figures to be entered by the Bidder" and other components should be left blank.

8.4 In case any column other than "Unit Rate (After discount, if any) In Figures to be entered by the Bidder" of Price Schedule is left blank, the value of that component shall be treated as inclusive in the unit price quoted.

8.5 Unit Price quoted must be exclusive of all duties and taxes. GST and Freight shall be quoted in the prescribed column of the BoQ. However, any other duties/levies may be quoted in column "Any other Levies/duties etc. for total quantity" and the details of such duties/levies shall be mentioned in the remark column.

8.6 In the case of revision of Statutory Levies/Taxes during the finalization period of tender, the purchaser reserves the right to ask for reduction in the prices if there is reduction in any duties or taxes.

8.7 A bid submitted with an adjustable or variable price will not be accepted.

8.8 The price approved by the purchaser for procurement will be inclusive of all levies and taxes i.e GST, packing, forwarding, freight and insurance etc., for delivery up to the Consignee. Break up/variation in various heads like Custom duty, GST, Insurance freight and other taxes paid/payable is for the information and any changes in the taxes shall have no effect on the price during the scheduled delivery period except that any decrease shall be passed on to the purchaser.

9.0 DOCUMENTS ESTABLISHING GOODS CONFORMITY TO BID DOCUMENTS:

9.1 The documentary evidence of goods in conformity with the Bid Documents may be in the form of literature and data and the bidder shall furnish a clause-by-clause compliance of all the terms & conditions of the tender demonstrating substantial responsiveness in the form of signing & stamping all the pages of the original bid document and supporting technical material by the authorized person/persons. In case of deviations, a statement of deviations and exceptions shall be given by the bidder.

9.2 For purposes of compliance to be furnished pursuant to Clause 9.1 above the bidder shall note that the standards for workmanship, material and

equipment and reference to brand names or catalogue number, designated by purchaser in its Technical Specifications are intended to be descriptive only and not restrictive.

9.3 The bidder should furnish the name of his OEM (if applicable), brand name, model no. and type of the products offered in this tender. The technical literature of the products should also be submitted. No change in either technology or product shall be permitted after opening of bids.

9.4 The bidder shall also furnish the technical literature of the offered products along with clause by clause compliance of the technical requirements mentioned in Section V of the tender document.

10.0 EARNEST MONEY DEPOSIT (BID SECURITY):

10.1 FURNISHING OF EMD

10.1.1 Earnest Money Deposit (refundable) as tabulated below is to be furnished with the bid by way of demand draft, banker's cheque, pay order, Fixed Deposit or Bank Guarantee (as per Annexure-IV) valid for at least 285 days, from the date of opening of bids, from any scheduled bank in India, drawn in favour of AO (Cash), TEC, payable at New Delhi. Any other amount of money lying with the purchaser cannot be adjusted against this head. Failure to furnish Earnest Money Deposit shall result in summarily rejection of the bid.

Sr. No.	Item	Type	Quantity	EMD (In Rupees)
1	Vulnerability Assessment tool (CVE Complied)	Testing tool	1	**55 Thousands**
2	Vulnerability Assessment tool (CCS 7 related)	Testing tool	1	**50Thousand**
3	Fuzzing tool (Ethernet Interface)	Testing tool	1	**30 Lakhs**
5	Static code Analysis and Dynamic Analysis Application Security Testing Tool)	Testing tool	1	**3.5Lakhs**
6	Binary Analysis Tool	Testing tool	1	**2.5 lakhs**
7	Penetration Testing Tool	Testing tool	1	**1.4 Lakhs**

In case the bidder quotes for more than one item, the EMD shall be sum of individual EMDs mentioned against those items in the above table and the list of item(s) for which EMD has been submitted, shall be uploaded on the portal along with scan copy of Demand Draft/Banker's Cheque/BG/FD.

10.1.2 The bidder registered with National Small Scale Industries Corporation (NSIC) for the tendered item(s) under single point registration scheme and desirous of claiming concessions available to such units inclusive of Earnest Money Deposit, should submit their latest and valid NSIC certificate and documents in respect of their monetary limit and financial capability duly certified by NSIC.

10.2 FORFEITURE OF EMD

The EMD shall stand forfeited if

a. The bidder withdraws its offer before initial bid validity.
b. The successful bidder, whose tender is accepted, fails or refuses to furnish the security deposit amount within the stipulated time, or fails or refuses to execute the contract.
c. It is established that near-relatives of bidder is working in the units of DoT, as detailed in this document.
d. In case it is found that tender document submitted by the bidder has been altered by way of tampering or doctoring.

In the above cases, the bidder will also not be eligible to participate in the tender in TEC for one year from the date of any of the above events.

10.3 REFUND/RELEASE OF EMD

10.3.1 No interest would be payable for any period on EMD or on any other amount lying with the purchaser.

10.3.2 The EMD amount/BG/FD will be refunded / released only after finalisation of tender from the unsuccessful bidders.

10.3.3 The EMD of the successful bidder will be refunded /released only after the receipt of the prescribed Performance Security Deposit.

11.0 PERIOD OF VALIDITY OF BIDS:

11.1 The prices quoted in the bid shall remain valid for acceptance by the purchaser for a period of 240 days from the date of opening of bids. A bid valid for a shorter period shall be rejected by the purchaser as non-responsive.

11.2 In case the Purchaser requests, in writing, the bidders to extend the period of validity of their bids, they may confirm the extension of the validity of their bids in writing, unconditionally. In such a case, the validity of the Bank Guarantee, if furnished, should also be extended suitably. A bidder may refuse the request without forfeiting its Earnest Money Deposit. A bidder accepting the request and granting extension will not be permitted to modify its bid.

12.0 SUBMISSION OF BIDS:

12.1 The bidders shall upload their bids online at e-procurement portal, in response to the e-tender published by the department. Bid submission can be done, as mentioned in the schedule in NIT (Section-I). 'Pre-Bid/Pre-Contract Integrity Pact', Indemnity Bond, EMD must be received by the Purchaser at the address Assistant Director General (MM), Room No. 257, TEC, Khurshid Lal Bhawan, Janpath, New Delhi not later than the prescribed

time on due date (1500 Hrs of 10.12.2021)**.** In case, the last date of submission of bids is declared as central government holiday in Delhi, the original EMD will be accepted up to the next working day till the same time and the Techno-commercial Bid will be opened on the next working day at the scheduled time.

12.2 The bidders should start the bid submission process well in advance so that they can submit their e-bid in time. The bidder should submit their e-bid considering the server time displayed in the e-procurement website. This server time is the time by which the e-bid submission activity will be allowed till the permissible time on the last/end date of submission indicated in the e-tender schedule.

12.3 Once the e-bid submission date and time is over, the bidders cannot submit their e-bid.

12.4 The Purchaser shall not be responsible for delay in submission of e-bid due to any reasons. No other mode of submitting the bid except the online method should be entertained

12.5 The Purchaser shall not be responsible if the bids are uploaded in any other portal than the one specified.

12.6 The Purchaser may, at its discretion extend this deadline for the submission of the bids by amending the tender document in accordance with Clause 5 of Section II in which case all rights and obligations of the Purchaser and bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

12.7 Not more than one bid shall be permitted from a single bidder otherwise all the bids submitted by such bidder shall be summarily rejected.

13.0 LATE BID:

The server time indicated in the bid management window on the e-procurement website http://eprocure.gov.in will be the time by which the e-bid submission activity will be allowed till the permissible date and time scheduled in the e-tender. Once the e-bid submission date and time is over, the bidder cannot upload the e-bid.

14.0 MODIFICATION AND WITHDRAWAL OF BIDS:

The bidder may modify, withdraw or re-submit its e-bid online only, before the bid submission date and time as per provisions available in CPP Portal.

15.0 OPENING OF BIDS:

15.1 A two stage process shall be adopted in the evaluation of the bids. The purchaser shall open Techno-commercial bids online and check the Techno-commercial bids proposal online.

15.2 Authorized Representatives may check the portal for status of tender opening, online.

15.3 The date fixed for the opening of bids, if subsequently declared as central government holiday in Delhi, the revised date of schedule will be notified. However, in absence of such notification, the bids will be opened in the next working day at the same time.

Stamp and signature of bidder

16.0 CLARIFICATION OF BIDS BY THE PURCHASER:

To assist in the examination, evaluation and comparison of bids, the purchaser may, at its discretion, seek clarification/document(s) of its bid from the bidder. Only the information furnished, by the bidder, shall be considered in future evaluation. However, no post-bid clarification at the initiative of any bidder shall be entertained.

17.0 TECHNO-COMMERCIAL BID EVALUATION:

17.1 The bids of only those bidders shall be considered for Techno-commercial evaluation, who have executed (in advance) and submitted the 'Pre-Bid/Pre-Contract Integrity Pact', on a stamp paper of Rs. 100, along with their bids. The authority to sign the Pact on behalf of the purchaser is ADG (MM), TEC. A copy of the signed pact shall be given to the bidder by the purchaser and the same will be uploaded on e-procurement portal along with the e-bid. The person signing the 'Pre-Bid/Pre-Contract Integrity Pact' should have authorization letter for signing the bid document as per clause no. 7.2.1(c) of Section II.

17.2 The bids will be evaluated Techno-commercially to determine whether they are complete, whether documents have been properly submitted, and whether bids are generally in order and qualify for opening and evaluation of financial bid.

17.3 Bid shall be considered substantially responsive if it conforms to the terms and conditions of the tender document without any material deviation.

17.4 The purchaser or his authorized representatives shall have the right to inspect the works, offices, showrooms, service centres etc. of the bidder, for verification of facts furnished by the bidder in support of his bid documents, and the bidder is bound to answer any query made by the purchaser.

17.5 During the preliminary examination, some minor infirmity and/or irregularity and/or nonconformity may also be found in some bids. Such minor issues could be a missing pages/attachment or illegibility in a submitted document. Such minor issues may be waived provided they do not constitute any material deviation. Wherever necessary, observations on such 'minor' issues (as mentioned above) may be conveyed to the bidder by CPP Portal/registered letter/speed post, and so on, asking him to respond by a specified date also mentioning therein that, if the bidder does not conform to purchaser's view or respond by that specified date, his bid will be liable to be rejected.

17.6 During evaluation of bids, the purchaser may, at his discretion, ask the bidder for clarifications on the bid. The request for clarification shall be given in writing through CPP Portal/registered/speed post, asking the bidder to respond by a specified date, and if the bidder does not comply or respond by the date, his bid will be liable to be rejected. The shortfall information/documents shall be sought only in case of historical documents which pre-existed at the time of the tender opening and which have not undergone change since then. These shall be called only on basis of the recommendations of the Tender Evaluation Committee. So far as the submission of documents is concerned with regard to qualification criteria,

after submission of the tender, only related shortfall documents shall be asked for and considered.

18.0 FINANCIAL BID OPENING/FINANCIAL EVALUATIONS AND COMPARISON OF BIDS:

18.1 The purchaser shall shortlist only those bidders who are eligible and have submitted substantially techno-commercially responsive bid for opening of financial bid. Successful bidders would be intimated regarding opening of financial bids. The Financial Bids of techno-commercially unsuccessful bidders would not be opened.

18.2 Prices quoted in the Price Schedule only will be considered for evaluation.

18.3 The evaluation and comparison of responsive bids shall be done on the total price of the quoted item(s), SLA charges for Annual Maintenance and, upgradation and SLA charges for services of professionals (wherever applicable) offered inclusive of Levies & Taxes i.e., GST, packing, forwarding, freight and insurance etc. as indicated in the Price Schedule.

18.4 The supplier shall quote for Service Level Agreement for 5 years after expiry of warranty period of 2 years. The cost shall be quoted as a lump sum for maintenance, Updates, Upgradation and visit of the engineers as and when required.

18.5 The purchaser may waive any minor infirmity or non-conformity or irregularity in a bid which does not constitute a material deviation, provided such waiver does not prejudice or affect the relative ranking of any bidder.

19.0 CONTACTING THE PURCHASER:

19.1 No bidder shall try to influence the purchaser on any matter relating to its bid, from the time of the bid opening till the time the contract is awarded.

19.2 Any effort by a bidder to influence the purchaser in the purchaser's bid evaluation, bid comparison or contract award decision shall result in the rejection of the bid of that bidder.

20.0 PURCHASER'S RIGHT TO ACCEPT ANY BID AND TO REJECT ANY OR ALL BIDS FOR INDIVIDUAL ITEMS:

The purchaser reserves the right to accept or reject any bid, and to annul the bidding process and reject all bids, at any time prior to award of contract without assigning any reason whatsoever and without thereby incurring any liability to the affected bidder or bidders on the grounds for the purchaser’s action.

21.0 PLACEMENT OF ORDER:

21.1 The purchaser shall consider placement of order(s) for commercial supplies on the bidder(s) whose offer has been found techno-commercially and financially acceptable. The tender will be awarded to the lowest (L-1) bidder of individual item.

21.2 The purchaser shall place an Advance Purchase Order of the tendered quantity on the bidder(s) whose offer has been accepted. The issue of an Advance

Purchase Order shall constitute the intention of the purchaser to enter into the contract with the bidder. The bidder(s) shall, within the stipulated time, furnish performance security in conformity with the terms and conditions, in the form of a demand draft or bank guarantee as per the proforma enclosed at Annexure VI, from any scheduled bank in India.

21.3 Failure to furnish performance security within the stipulated time may result in cancellation of Advance Purchase Order along with forfeiture of the EMD.

21.4 Purchase Order will be placed only after acceptance of the performance security submitted by the bidder.

21.5 The issue of Purchase Order shall constitute the Award of Contract on the bidder(s).

22.0 PURCHASER'S RIGHT TO VARY QUANTITIES AT TIME OF AWARD:

22.1 Purchaser reserves the right at the time of award of contract to increase or decrease of item(s) by one unit and services specified in the Schedule of Requirements as per requirements of the purchaser without any change in unit price of the ordered quantity or other terms and conditions at the time of award of contract.

22.2 **Repeat Order:** The purchaser reserves the right to place repeat order of additional one unit during one year from the date of First Purchase Order. However, such orders shall be placed after price negotiation (downward) with the supplier considering the reasonability of rates based on prevailing market conditions and the impact of reduction in duties and taxes etc.

23.0 DISQUALIFICATION OF BIDDER:

23.1 Purchaser reserves the right to disqualify the bidder for a period as deemed fit to the purchaser who have habitually failed to supply the equipment in time. Further, the suppliers whose equipment does not perform satisfactorily in accordance with the specifications may also be disqualified for a period as deemed fit to the purchaser.

23.2 Purchaser reserves the right to blacklist a bidder for a period as deemed fit to the purchaser, in case bidder fails to honour his bid without sufficient grounds.

23.3 The bidder should give a certificate that none of his/her near relatives is working in the units where he/she is going to apply for the tender, as per Annexure-V. None of the near relatives of proprietor OR all partners of partnership OR all the Directors of the company excluding Government of India/Financial institution nominees and independent non-Official part time Directors appointed by Govt. of India or the Governor of the state should be working in the unit where the tender is being applied. The near relatives for this purpose are defined as: -

a. Members of a Hindu undivided family.
b. They are husband and wife.
c. The one is related to the other in the manner as father, mother, son(s) & Son's wife (daughter in law), Daughter(s) and daughter's husband (son in law), brother(s) and brother's wife, sister(s) and sister's husband (brother in law).

Stamp and signature of bidder

23.4 Due to any breach of conditions as mentioned in clause 23.2 and 23.3 by the company or firm or any other person the bid will be cancelled and Earnest Money Deposit will be forfeited at any stage whenever it is noticed and purchaser will not pay any damage to the company or firm or the concerned person. The company or firm or the person will also be debarred for further participation in the concerned unit.

Stamp and signature of bidder

SECTION - III
GENERAL (COMMERCIAL) CONDITIONS OF CONTRACT

1.0 APPLICATION:

The General Conditions shall apply in contracts made by the purchaser for the procurement of Goods and associated services.

2.0 STANDARDS:

The Goods supplied under this contract shall conform to the standards prescribed in the Technical Specifications mentioned in Section-V & Special conditions mentioned in Section IV.

3.0 PATENT RIGHTS:

The Supplier shall indemnify, in the format prescribed in Annexure-II, the purchaser against all third-party claims of infringement of patent, trademark or industrial design rights arising from use of the goods or any part thereof in Indian Telecom Network & TEC Laboratory.

4.0 PERFORMANCE SECURITY:

4.1 The contractor shall furnish performance security to the purchaser for an amount equal to 3% of the Contract Price (including training, SLA, accessories and accreditation) for the item(s) as prescribed in Advance Purchase Order within 15 days of issue of the Advance Purchase Order.

4.2 The proceeds of the performance security shall be payable to the purchaser for non-compliance on account of the contractor's failure to complete its obligations under the contract.

4.3 The performance security may be submitted in the form of demand draft in favour of AO (Cash), TEC, or in the form of a Performance Bank Guarantee (PBG) issued by a scheduled bank and in the proforma provided in 'Annexure-VI' of this tender document.

4.4 The Performance Bank Guarantee (PBG) shall be valid for at least 7 years & 6 Months from the date of Advance Purchase Order. The PBG shall be renewed from time-to-time till all the liabilities of the supply of goods and services are resolved by the contractor, or till 6 months beyond the expiry of SLA period of supply, whichever is later.

4.5 In case, any amount of Liquidated Damages (L/D) is recovered from PBG, the Contractor shall replenish the PBG to original value within 30 days of recovery.

4.6 The purchaser will discharge the performance security bond, deducting the pending dues, liquidated damages, if any, after completion of the contractor's performance obligations including warranty obligations under the contract.

4.7 No interest shall be paid on the security deposit amount.

5.0 INSPECTION AND TESTS:

5.1 The purchaser or his representative shall have the right to inspect and test the item(s) for their conformity to the specifications. Where the purchaser decides to conduct such tests on the premises of the OEM(s), all reasonable facilities and assistance like Testing instruments, hardware and other test gadgets and relevant software & software test scripts including access to drawings and production data shall be furnished to the inspectors at no charge to the purchaser.

5.2 Should any inspected or tested item(s) fail to conform to the Specifications the purchaser may reject them and the Supplier shall either replace the rejected item(s) or make all alterations necessary to meet Specification requirements free of cost to the purchaser.

5.3 Notwithstanding the pre-supply tests and inspections prescribed in 5.1 & 5.2 above, the equipment and accessories on receipt in the purchaser's premises will also be tested during and after installation before "take over" and if any equipment or any part thereof is found defective, the same shall be replaced free of all cost to the purchaser as laid down in clause 5.4 below.

5.4 If any equipment or any part thereof, before it is taken over under clause 5.5 below, is found defective or fails to fulfil the requirements of the contract, the inspector shall give the Supplier notice setting forth details of such defects or failure and the Supplier shall make the defective equipment good, or alter the same to make it comply with the requirements of the contract forthwith and in any case within a period not exceeding three months of the initial report. These replacements shall be made by the Supplier free of all charges at site. Should it fail to do so within this time, the purchaser reserves the discretion to reject and replace at the cost of the Supplier the whole or any portion of the equipment as the case may be, which is defective or fails to fulfil the requirements of the contract. The cost of any such replacement made by the purchaser shall be deducted from the amount payable to the Supplier.

5.5 When the acceptance testing of an item(s) is completed, respective item(s) of SECURITY TEST Lab will be declared as commissioned and the Inspector/Consignee will issue a Taking Over Certificate. The Inspector / consignee shall not delay the issue of any "Taking Over Certificate" contemplated by this clause on account of minor defects in the physical installation which do not materially affect the commercial use thereof provided that the supplier shall undertake to make good the same in a time period not exceeding three months. The Taking Over Certificate shall be issued by the consignee within three weeks of commissioning of respective item(s) of SECURITY TEST Lab. In this case BCPC (Bill copy payable challan) shall be equivalent to "Taking over certificate" issuance of which shall certify receipt of goods in Safe & Sound Condition. However, they shall not discharge the supplier of their warranty obligation.

5.6 Nothing in clause 5 shall, in any way release the Supplier from any Warranty or other obligations under this contract.

6.0 PACKING, FORWARDING AND DISPATCH DOCUMENTS:

6.1 The contractor shall ensure that the goods are securely and adequately packed and marked to ensure safe arrival at the destination withstanding all

hazards, such as rough handling severe climatic conditions, natural calamities etc. during transit.

6.2 The contractor shall be fully responsible for the safe arrival of the goods at destination and till the time they are received by the consignee, in good working condition.

6.3 Intimation of dispatch of goods should be sent to the consignee well within time. Such intimation should also be sent to the paying authority and to the purchaser.

6.4 The goods shall be supplied in original packing from the manufacturer clearly indicating item's Serial No, date, etc.

7.0 DELIVERY:

7.1 The supplier shall warrant that the stores / equipment (including software and software tools) or any part thereof to be supplied shall be new and free from all defects and faults in materials used, workmanship and manufacture and shall be of the highest grade and consistent with the established and generally accepted standards for materials of the type ordered and shall perform in full conformity with the technical specifications and drawings as per Section V.

Delivery of the goods along with original printed copies of instruction/ operation manual(s) in English, test reports for hardware and software, software licences and documents shall be made by the Contractor in accordance with the Schedule of Requirements (SOR) and the Special Conditions of the contract. The delivery of the equipment shall be to the Consignee as given in the purchase order. OEM Quality Check Certificate would be required along with item(s).

7.2 The delivery of the goods and documents should be implemented strictly as per the delivery schedule. All the goods are to be delivered at the location specified in the Purchase Order.

7.3 The schedule for delivery, installation and acceptance testing shall be as follows:

S No.	Target	Timeline
1	Supply of Item(s)	40 days from date of placement of respective PO
2	Installation	60 days from date of placement of respective PO or 20 days from supply of item(s), whichever is later
3	Acceptance testing	120 days from date of placement of respective PO or 60 days from completion of installation, whichever is later as per Clause 5 of **Section-IV**.

7.4 In case the purchaser exercises the right of pre supply testing as per clause 5.1 of Section III, supplier has to ensure that the item(s) are offered for pre-supply testing sufficiently in advance so as to meet the scheduled delivery

Stamp and signature of bidder

requirement. Purchaser shall not be responsible in any manner for deviation from the prescribed delivery schedule.

7.5 The supplier shall provide original licenses from its OEM for all software.

7.6 If the supplier fails to complete the supply, installation and acceptance testing as per clause 7.3 above, the purchaser reserves the right to cancel the P.O. and en-cash the Performance Bank Guarantee.

7.7 The extension of delivery period against the purchase order, if any, may be granted subject to the condition that purchaser shall have the absolute right to revise the price(s) as per clause 10 of Section III and also to levy penalty for the delayed supplies.

8.0 WARRANTY:

8.1 The supplier shall warrant that the stores / equipment (including software and software tools) or any part thereof to be supplied shall be new and free from all defects and faults in materials used, workmanship and manufacture and shall be of the highest grade and consistent with the established and generally accepted standards for materials of the type ordered and shall perform in full conformity with the technical specifications and drawings as per Section V. The supplier shall be responsible for any defect that may develop under the conditions provided by the contract and under proper use, arising from faulty material, design or workmanship such as corrosion of the equipment, inadequate quality of material to meet equipment requirements, inadequate contact protection, deficiencies in circuit design and/or otherwise and shall remedy such defects at his own cost when called upon to do so by the purchaser who shall state in writing in what respect the stores are faulty. This warranty shall survive inspection or payment for / and acceptance of goods, but shall expire (except in respect of complaints notified prior to such date) 24 months after the commissioning of respective item(s) of Lab as mentioned in Clause 5.1 of Section IV. The warranty period of the hardware and software components shall be for two years after successful commissioning. During the warranty period, the complete responsibility to keep the equipment working (including manpower (wherever applicable) and replacement of parts / components hardware and software and or both) shall rest with the supplier

8.2 If it becomes necessary for the Supplier to replace or renew any defective portion(s) of the equipment under this clause, the provisions of the Clause 5.4 of this Section shall apply to the portion(s) of the equipment so replaced or renewed or until the end of the above mentioned period of 24 months, whichever may be later. If any defect is not remedied by the supplier within two weeks, the Purchaser may proceed to get the defects remedied from other sources, at the supplier's risk and expenses, but without prejudice to any other rights which the purchaser may have against the supplier in respect of such defects including extension of warranty for delay beyond 2 weeks. SLA conditions as per Section IV shall be applicable during warranty period also except that no payment shall be made for compliance of SLA conditions during warranty period.

8.3 Replacement of any hardware and software components under warranty clause shall be made by the supplier free of all charges at site including freight, insurance and other incidental charges.

9.0 PAYMENT TERMS:

9.1 (I) The terms of payment for all the items (except Fuzzer-E) stated in Price Schedule, excluding Annual Maintenance SLA cost will be as under:

a) 30% payments shall be released on proof of receipt of ordered Security tool(s) and associated hardware by the consignee as certified by acceptance Testing Committee.

b) 30% payment shall be released on installation of the ordered individual Security tool.

c) 30 % payment on completion of acceptance testing of individual Security tool.

d) Balance 10% of payment shall be released on first EUT (Equipment Under Test) testing or 90 days after acceptance testing, whichever is earlier after adjusting LD for non-compliance. This payment shall be released only after the release of payment of all the above stages (a to c).

(II) The terms of payment for Fuzzer-E, stated in Price Schedule, excluding Annual Maintenance SLA cost will be as under:

a) 15% payments shall be released on proof of receipt of ordered Security tool and associated hardware material by the consignee as certified by acceptance Testing Committee.

b) 15% payment shall be released on acceptance testing of protocol list A in Annexure IX.

c) 60% payment on completion of acceptance testing of protocol list B in Annexure IX. The supplier can claim this payment on pro-rata basis upon acceptance testing of protocols in List B in steps of 10%.

d) Balance 10% of payment shall be released on first EUT testing after adjusting LD for non-compliance. This payment shall be released only after the release of payment of all the above stages (a to c).

9.2 Cost of the item(s) supplied as per purchase order will be paid on receipt of the item(s) in good condition by consignee, at site on production of following documents:

a. Bills in duplicate duly pre-receipted
b. Delivery Challan
c. Custom Duty Paid Certificate or equivalent document if applicable.
d. Certificates of receipt of goods in physically good condition from the consignee.

9.3 Payments would be made in Indian Rupees. Any foreign Exchange & Customs clearance formalities if necessary will have to be arranged by the supplier himself.

10.0 PRICES:

10.1 Prices charged by the supplier for goods delivered and services performed under the contract shall not be higher than the prices quoted by the Supplier in his Bid.

10.2 Prices once fixed will remain valid during the scheduled delivery period. Any changes in the taxes shall have no effect on the price during the scheduled delivery period except that any decrease shall be passed on to the purchaser.

10.3 Any increase in taxes and other statutory duties/levies after the expiry of the delivery date shall be to the supplier's account. However, benefit of any decrease in these taxes/duties shall be passed on to the purchaser by the supplier.

11.0 SUBCONTRACTS:

No subcontracts are permitted.

12.0 DELAYS IN THE SUPPLIER'S PERFORMANCE:

12.1 Delivery of the Goods and performance of the services shall be made by the Supplier in accordance with the time schedule specified by the purchaser in its purchase order. In case the supply is not completed in the stipulated delivery period, as indicated in the Purchase Order, purchaser reserves the right to short close/cancel this purchase order and/or recover liquidated damage charges. The cancellation/short closing of the order shall be at the risk and responsibility of the supplier and purchaser reserves the right to purchase balance unsupplied item(s) at the risk and cost of the defaulting suppliers.

12.2 Delay by the Supplier in the performance of its delivery and SLA obligations shall render the Supplier liable to any or all of the following sanctions, viz., imposition of liquidated damages, and forfeiture of its performance security and/or termination of the contract for default.

12.3 If at any time during the performance of the contract, the supplier encounters condition impacting timely delivery of the goods and performance of service, the Supplier shall promptly notify to the purchaser in writing the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the supplier's notice, the purchaser shall evaluate the situation and may at its discretion extend the period for performance of the contract subject to extension of period of performance security deposit. The extension of period for performance so granted will include extension of warranty/or SLA period also.

12.4 If the supplies are not completed in the extended delivery period, the purchase order may be short-closed and the Performance Security shall be forfeited. However, in such situation the supplier will have to furnish a fresh performance security of 10% of the Purchase Order value for the quantity supplied.

12.5 In case the partner OEM fail to support/help the supplier and as a result bidder fails to provide satisfactory service to the TEC, the supplier alone will be held liable for any kind of loss incurred by the TEC.

13.0 LIQUIDATED DAMAGES:

13.1. The date of delivery of the stores stipulated in the acceptance of tender should be deemed to be the essence of the contract and delivery must be completed not later than the dates specified therein. Extension will not be given except in exceptional circumstances. Should, however, deliveries be made after expiry of the contract delivery period, without prior concurrence of the

purchaser, and be accepted by the consignee, such deliveries will not deprive the purchaser of his right to recover liquidated damages under clause 13.2 below. However, when supply is made within the contracted original delivery period, the consignee may accept the stores and in such cases the provision of clause 13.2 below will not apply.

13.2. Should the supplier fail to deliver the stores or any consignment thereof within the period prescribed for delivery the purchaser shall be entitled to recover 0.5% of the value of the delayed supply for each week of delay or part thereof for a period upto 10 weeks and thereafter at the rate of 0.7% of the value of the delayed supply for each week of delay or part thereof for another 7 weeks of delay.

13.3. Further if there is a delay in installation or acceptance testing, LD charged shall be levied on the total value of the Purchase Order (excluding the value of Annual Maintenance SLA). The LD rate shall be 0.5% of total value per week for period of ten weeks and thereafter at the rate of 0.7% of the total value per week for each week of delay or part thereof for another 7 weeks of delay.

13.4. Quantum of liquidated damages assessed and levied by the purchaser shall be final and not challenged by the supplier. LD if any will be recovered from the payment to be made to the supplier.

13.5. Any amount which becomes due and recoverable from the contractor on account of liquidated damages or account of any matter relating to this contract, shall also be recoverable from any sum that is due or any sum thereafter may become due to the contractor out of this contract or any other contract with the Government.

13.6. The PBG shall be encashed to the extent of LD amount, if the same is not paid within the time period specified in the notice for recovery of LD. Where the Bank Guarantees have been encashed partially, the supplier on such occasions shall restore the encashed guarantees to the full amount. Any failure to do so shall amount to violation of the terms and conditions of the project. Without prejudice to its rights of any other remedy, purchaser may encash Bank Guarantee (PBG) in case of any breach in terms & conditions of the Contract by the supplier.

14.0 FORCE MAJEURE:

14.1 If, at any time, during the continuance of this contract, the performance in whole or in part by either party of any obligation under this contract is prevented or delayed by reasons of any war or hostility, acts of the public enemy, civil commotion, sabotage , fires, floods, explosions, epidemics, quarantine restrictions, strikes, lockouts or act of God (hereinafter referred to as events) provided notice of happenings of any such eventuality is given by either party to the other within 21 days from the date of occurrence thereof, neither party shall by reason of such event be entitled to terminate this contract nor shall either party have any claim for damages against other in respect of such non-performance or delay in performance, and deliveries under the contract shall be resumed as soon as practicable after such an event come to an end or cease to exist, and the decision of the purchaser as to whether the deliveries have been so resumed or not shall be final and conclusive. Further that if the performance in whole or part of any obligation

under this contract is prevented or delayed by reasons of any such event for a period exceeding 60 days, either party may, at its option, terminate the contract.

14.2 Provided, also that if the contract is terminated under this clause, the purchaser shall be at liberty to take over from the Supplier at a price to be fixed by the purchaser, which shall be final, all unused, undamaged and acceptable materials, bought out components and stores in course of manufacture which may be in possession of the Supplier at the time of such termination or such portion thereof as the purchaser may deem fit, except such materials, bought out components and stores as the Supplier may with the concurrence of the purchaser elect to retain.

15.0 TERMINATION FOR DEFAULT:

15.1. The purchaser may, without prejudice to any other remedy for breach of contract, by written notice of default, sent to the supplier, terminate this contract in whole or in part

a. If the supplier fails to deliver any or all of the goods within the time period(s) specified in the contract, or any extension thereof granted by the purchaser pursuant to Clause 12.3 of this section.
b. If the supplier fails/delays to perform any other obligation(s) under the Contract; and
c. If the supplier, in either of the above circumstances, does not remedy his failure within a period of 15 days (or such longer period as the purchaser may authorize in writing) after receipt of the default notice from the purchaser.

15.2. In the event the purchaser terminates the contract in whole or in part pursuant to Clause 15.1 the purchaser may procure, upon such terms and in such manner as it deems appropriate, goods similar to those undelivered and the supplier shall be liable to the purchaser for any excess cost for such similar goods. However, the supplier shall continue the performance of the contract, including SLA, to the extent not terminated.

16.0 TERMINATION FOR INSOLVENCY:

The purchaser may at any time terminate the Contract by giving written notice to the Supplier, without compensation to the supplier, if the supplier becomes bankrupt or otherwise insolvent as declared by the competent court provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the purchaser.

17.0 ARBITRATION:

17.1 In the event of any dispute or difference arising as to the execution of the contract or as to the respective rights or liabilities of the parties or the interpretation of any condition of agreement (except as to any matters the decision of which is specially provided for any by those or the special conditions) the same shall be referred to the sole arbitration of Advisor (O), DoT, New Delhi or of his nominee. If the post of Advisor (O) is vacant, a higher authority or his nominee will act as Sole Arbitrator. The award of the arbitrator shall be final and binding on the parties to the agreement.

17.2 The arbitrator may from time to time with the consent of the parties to the agreement enlarge the time for making the award.

17.3 Upon every such reference, the assessment of the cost incidental to the reference and award respectively shall be the discretion of the arbitrator.

17.4 The agreement to appoint an arbitrator will be in accordance with the Arbitration and Reconciliation Act. 1996.

17.5 In the event of such arbitrator to whom the matter is originally referred, being transferred or vacating his office or being unable to act for any reasons whatsoever another person shall be appointed to act as arbitrator by purchaser in accordance with terms of agreement and person so appointed shall be entitled to proceed from the stage at which it was left out by his predecessors.

17.6 The venue of arbitration shall be New Delhi the place from which the acceptance note is issued or such other places, as the Advisor (O) at his discretion may determine. In this clause, the terms Advisor (O) includes any other officer who is for the time being discharging the duties of Advisor(O), whether in addition to other functions or otherwise.

18.0 SET OFF:

Any sum of money payable to the contractor (including security deposit refundable to him) under this contract may be appropriated by the purchaser or the purchaser or any other person or persons contracting through the purchaser and set off the same against any claim of the purchaser or purchaser or such other person or persons for payment of sum of money arising out of this contract or under any other contract made by the Contractor with purchaser of the purchaser or such other person or persons contracting through the purchaser.

19.0 COURT JURISDICTION:

This Contract/PO is subject to jurisdiction of the competent Courts at New Delhi only.

20.0 PAYMENT METHOD:

20.1 Payment shall be made to the contractor electronically or through cheque for which a supplier shall provide the necessary details of his bank account.

20.2 Income Tax or any other applicable taxes shall be deducted at source at the time of payment to the contractor, in accordance with the provisions of the relevant applicable Acts.

21.0 PAYING AUTHORITY:

Sr. DDG (TEC), shall be the paying authority and A.O. (Cash), Telecommunication Engineering Centre, Gate No. 5, Khurshid Lal Bhavan, Janpath, New Delhi will be the disbursing authority.

22.0 CONSIGNEE AND OFFICER IN CHARGE:

ADG (AS), Telecommunication Engineering Centre, Gate No. 5, Khurshid Lal Bhavan, Janpath, New Delhi shall be Consignee for receipt of materials. ADG (TS), TEC or the authority designated by the purchaser will be the officer in-charge for the complete project.

Stamp and signature of bidder

SECTION - IV
SPECIAL CONDITIONS OF CONTRACT

1.0 The special conditions of contract shall supplement the 'Instructions to the Bidders' as contained in Section II & "General (Commercial) Conditions of the Contract" as contained in Section III and wherever there is a conflict, the provisions herein shall prevail over those in Section II and Section III. If there is any discrepancy in NIT and eligibility, terms & conditions stipulated in tender document, provision in the tender documents will prevail. For interpretation of any condition of this tender document, the decision of Purchaser shall be final and binding on the Bidder.

1.1 The bidder shall furnish the name of his respective OEM (if applicable), brand name, type of license, model no./version no and type of the products offered in this tender. The technical literature of the products should also be submitted. No change in either technology or product shall be permitted after opening of bids except for the upgraded version of that product with the prior approval of the purchaser.

1.2 The supplier with regard to item supplied will comply with applicable PMI directive (Preference to Make in India) issued by Government of India subject to meeting of Technical and Commercial conditions of Contract.

2.0 Turnkey Project:

The Supplier shall be responsible for the complete supply, installation, acceptance testing and commissioning of individual testing tool(s)/lab infrastructure item(s) for which the bidder has quoted under this tender. All DUTs (Device under Test) and /or software required for the purpose of completing the acceptance testing shall be arranged by the supplier at no extra cost to purchaser.

2.1 Supplier's Responsibilities:

The responsibility of the Supplier shall be as follows:

a. Supply, installation, acceptance testing, operation (if applicable) & maintenance of tools, related hardware with accessories and accreditation support.

b. Supply and installation of spare parts, and special tools, etc., whenever required.

c. Providing set of complete documents for respective tool(s) and lab infrastructure item(s). This shall include physical and wiring layout, network diagrams and operation and maintenance documents

d. To conduct the required initial training and two more in-house trainings during the contract period as per requirement of Purchaser.

e. The Supplier shall provide the peak power requirements and heat load of the equipment's / tools in technical bid.

f. The Supplier shall provide fireproof cabling.

g. The SUPPLIER shall depute fully competent and responsible Professionals at the Security test lab initially for installation till end of

warranty period for (i) penetration testing tool and (ii) Static code Analysis and Dynamic Analysis Application Security Testing Tool)with no associated liability on the purchaser. The Professionals shall have at least one year of hands on experience on the respective tools and atleast 2 years' experience in Information Security and shall be certified by GIAC/ISCII/ISASCA/CWNP or any other equivalent security certification. He/She shall be well verse in running tools being supplied to meet the scope of the SECURITY TEST Lab. Professionals shall be capable of giving all types of required technical guidance/assistance to the In-charge & staff of Security test lab in respect of configuration, creation of test scripts as applicable, testing DUT/EUT and reporting results.

h. Purchaser reserves the right to ask for the change of Professional deployed in case of unsatisfactory performance which must be complied within two weeks from the request made by the purchaser.

2.2 **ROLE OF Purchaser:**

Role of Purchaser shall be to provide the following:

a. Necessary infrastructure including Power backup and air-conditioned working space in the premises of purchaser.

b. Space for installation of equipment in purchaser building.

c. Facilities like AC electric power etc. for which planning and deployment shall be separately done for the SECURITY TEST lab required. The supplier shall provide all infrastructure requirements in Technical proposal.

d. Necessary lab infrastructure like Racks and furniture shall be arranged by Purchaser.

3.0 Complete System:

The intention of this specification is basically to specify the main features required for the Security Test lab. The bidder is required to provide complete details of additional facilities/optional facilities available in the offered Security tools even though they may not be covered by these specifications. The list of specifications indicated in the Tender Document is indicative only.

4.0 Project schedule:

The supplier shall submit a detailed project execution plan within 15 days of issue of purchase order complying the clause 7.3, Section III, mentioning all activities like supply, installation and acceptance testing of the testing tool(s) and lab infrastructure item(s) of SECURITY TEST lab and abide by it.

5.0 Installation, Acceptance Testing, Commissioning, Operations & Maintenance:

5.1 It shall be the responsibility of the Supplier to install and successfully complete acceptance testing of the testing tool(s) and lab infrastructure item(s) including hardware and software within the specified period of time. It shall be ensured that all the necessary equipment is delivered in time.

Stamp and signature of bidder

The testing tool(s) and lab infrastructure item(s) shall be considered commissioned after acceptance testing by purchaser.

5.2 **For the purpose of supply and acceptance testing of SECURITY TEST lab project the following terms shall be used:**

Device under Test (DUT): The set of DUTs to be arranged by the supplier for the purpose of acceptance testing of respective testing tool of SECURITY TEST Lab. For Fuzzer, DUT within the scope of this document shall mean set of equipment, software and tools in which protocols of List A of Fuzzer-E of Annexure IX are supported and can be verified.

Equipment under Test (EUT): The equipment offered for testing to TEC after acceptance testing.

5.3 The testing tools of SECURITY TEST Lab shall be treated as commissioned on completion of following activities:

a. Installation, acceptance testing (acceptance testing as per the test schedule approved by the purchaser) with DUTs. In case of non-availability of DUTs, the simulators can be used to demonstrate acceptance testing.
b. Acceptance testing of LIST A of Annexure IX for Fuzzer-E, as per clause 9.1 of this Section.
c. Upgradation of the tools (if applicable),
d. Updation of the tools.
e. Verification of stock including spares, softwares and its licences.

In addition to above, there shall not be any pending performance and availability issues. At the same time performance of the professional(s) for respective tool, i.e. (i) penetration testing tool and (ii) Static code Analysis and Dynamic Analysis Application Security Testing Tool), positioned in the lab by the supplier should have been satisfactory as judged by the purchaser.

5.4 Onsite support of domain expert professionals for following testing tools shall be made:

S No.	Tools	Duration
1	Static code Analysis and Dynamic Analysis Application Security Testing Tool)	From installation till end of warranty period
. 2	Penetration Testing Tool	From installation till end of warranty period

Note: Professional service charges, for the warranty period, may be quoted separately for items mentioned at S. No. 1 & 2. The supplier must ensure the availability of trained professionals on a daily basis. However, TEC reserves the right to extend the service of professionals as and when required after the expiry of warranty period on the quoted rate.Professional service charges, for the contract period, may be quoted separately for items mentioned at S. No. 1 & 2. The supplier must ensure the availability of trained professionals on a daily basis.

6.0 Acceptance testing:

6.1 The acceptance testing of the Security Test lab tools shall be carried out by a committee constituted by the purchaser at the installation / purchaser site. The supplier shall be required to give a detailed test plan for the equipment supplied within fifteen days of the placement of PO. The test plan shall cover testing of various DUTs along with its OS, networking software and application software. The test plan shall also cover all the tools that are being supplied to meet the scope and objective of the SECURITY TEST Lab. The test plan shall be approved by the purchaser with modifications as deemed fit and the same shall be final. The test plan shall include the hardware (the entire technical requirement mentioned in the specification) and the software related tests. Purchaser reserves the right to conduct certain tests, wherever offered, at any site other than the installation site. The supplier shall make necessary arrangements to facilitate smooth testing of the offered equipment. Delay in submission of test plan and acceptance testing of respective testing tool and lab infrastructure item(s) of SECURITY TEST Lab shall result in LD as per clause 13 of Section III.

6.2 Non-completion of acceptance testing shall not prevent the purchaser to use the lab for commercial purpose.

6.3 If there is any delay in completion of acceptance testing beyond prescribed time, the supplier shall provide support as applicable during warranty period without any cost to the purchaser. Any non-compliance to these obligations as per clauses 5 & 12 of this section and clause 8 of Section III will lead to LD's/actions as per terms & conditions mentioned in the tender document. This shall not constitute start of warranty period as per clause 12 of this Section.

7.0 TRAINING:

7.1 The supplier shall submit a generic initial training/lecture plan with names of topics proposed to be covered along with the acceptance of APO. The purchaser will finalise the training schedule including the contents of the training which will be binding on the supplier. The training shall commence within six weeks after placement of PO.

7.2 The initial training shall be for at least ten persons at the established centres of the respective OEMs by the employees of OEMs. The training will be provided without any extra cost to the purchaser. The transport/boarding/lodging expenses of the trainees will be borne by the purchaser. All other costs, including that of trainer, training material, training tools/aids and generation/evaluation of test reports, will be borne by the supplier.

7.3 Initial training shall be followed by two onsite trainings for at least 10 persons within two years of the commissioning of respective testing tools of SECURITY TEST Lab. Delay in providing onsite training shall result in extension of warranty. The training requirement for initial and 2 onsite trainings each for various tools are as follows:

S No.	Tools	Duration (in days) for total 3 trainings(minimum)
1	Vulnerability Assessment tool (CVE Complied)	6
2	Vulnerability Assessment tool (CCS 7 related)	6
3	Fuzzing tool (Ethernet Interface)	9
4	Static code Analysis and Dynamic Analysis Application Security Testing Tool)	6
5	Binary Analysis Tool	6
6	Penetration Testing Tool	9

7.4 Training material, in the form of high quality printed documents and/or in the form of soft copy, shall be provided by the contractor to every trainee. One set of training material shall also be given to consignee and ADG (MM), TEC both. The training material would be standard, which the OEMs provide to their other clients globally. The purchaser reserves the right to reject training material, if not found of proper quality. In such a case the supplier shall immediately replace rejected material with good quality material.

7.5 The training shall include class room and hands on practical sessions on the following:

i. Installation and Configuration of the respective testing tool(s) (including hardware and software)
ii. Operation and Maintenance of the respective testing tool(s) (including hardware and software)
iii. Testing procedure for different Applications Software/ Networking Software / Operating System
iv. Day to day maintenance and up gradation of testing tool(s).

8.0 TAKING OVER OF THE TESTING TOOL(S) AND LAB INFRASTRUCTURE ITEM(S) OF SECURITY TEST LAB:

The testing tool(s) of SECURITY TEST Lab shall be taken over by the consignee on fulfilment of the following conditions:

a) Commissioning of respective testing tool(s) of SECURITY TEST Lab as defined in clause 5.3 of this Section.

b) Imparting initial training as per clause 7 above.

9.0 UPDATES:

9.1 All software features provided initially with various tools including protocols listed in LIST A and B in Annexure IX of the tender document shall fall within the purview of updates.

9.2 The supplier shall provide correction patch for any software bug, noticed from the date of supply till the end of contract, in the supplied software, at no extra cost to the purchaser. This shall also cover updates as per

Stamp and signature of bidder

3GPP/3GPP2/IETF/ITU-T/MEF/Broad Band forum/IPv6 Forum/any other protocol already mentioned in the technical conditions specified under Section V, at no extra cost to the purchaser.

9.3 Update in VA tool shall be done on weekly basis. For VA tools the updates shall be done in complete synchronization with the vulnerabilities published in catalogue (CVE/NVD/any other telecom vulnerabilities catalogue) update. In case, purchaser requests update of VA tool because of declaration of any special vulnerability, VA tool shall be updated within 2 days. LD charges for delay in updation shall be Rs 1000 per day for first two days followed by Rs 5000 per day.

9.4 Any media used for upgradation and updates shall remain within the SECURITY TEST Lab premises.

10.0 UPGRADATION:

10.1 The project envisages supply, installation, acceptance testing, commissioning, and two-year warranty after commissioning and there after five years of Annual Maintenance support as per SLA for the respective item(s) of the SECURITY TEST lab in TEC.

10.2 The supplier shall quote cost of Annual Maintenance Service Level Agreement(SLA) as detailed in Price Schedule. The scope shall broadly include:

A. Services for Annual Maintenance which will also include cost of update/upgradation as per 3GPP/3GPP2/IETF/ITU-T/MEF/Broad Band forum/IPv6 Forum/any other protocol for Fuzzer and cost of upgradation of other tools for the entire duration of Contract.
B. Upgrade/Repair/replacement cost of associated hardware of the security tool to meet desired performance.

The detailed scope may be seen in Clause 11 of this Section.

10.3 Upgradation of various tools shall also mean any new feature developed by the OEM which is not covered in clause 9 of this section. The upgrade requirement of various tools shall be as per Section V (TECHNICAL SPECIFICATIONS & SCHEDULE OF REQUIREMENT).

10.4 Keeping the lab up-to-date by way of timely upgradation and updates is very crucial for this project.

10.5 Upgradation of the tools shall be intimated by the supplier within one week from the date of release.

10.6 Any hardware, software, firmware which is required as a pre-requisite to support upgradation shall be provided free of cost. Any specific training to utilize the upgraded feature shall be provided on site by the supplier at no extra cost to the purchaser.

10.7 Updates and Upgrades shall not be allowed remotely. Separate platform shall be provided for updates and upgrades. Remote supervision of SECURITY TEST Lab tool(s) and lab infrastructure item(s) shall not be permitted.

10.8 LD charges of Rs Ten thousand per week or part thereof shall be levied in case of delay in upgradation of testing tools of the SECURITY TEST lab as per the requirement of clause 10.1 to 10.7 above. In case the tools are under

use to test offered EUT and their non-updation and non-upgradation is hampering the testing activities, LD shall be Rs five thousand per calendar day of delay.

11.0 Annual Maintenance SERVICE LEVEL AGREEMENT (SLA):

The SLA will come into force immediately after completion of warranty period and shall be valid for five years. No separate SLA agreement will be signed as the same will be part of the Purchase Order itself.

11.1 During the period of SLA, the Supplier shall inter alia:

i Diagnose the hardware and software faults.

ii Rectify the hardware and software faults.

iii Repair and replace the faulty PCB/modules and any other equipment or part thereof.

iv Carry out the periodic preventive maintenance on quarterly basis or as recommended by OEM's of the tools.

v Supply all software updates on continuing basis.

vi Perform Software maintenance like software debugging, patch implementation, version control of software, document generation and repository of working versions.

vii Software upgrades and new software versions, of the new releases/ upgrades of - various standards, specifications, recommendations, etc. (of ITU, IETF, ETSI, IEEE, 3GPP, 3GPP2, MEF, IPv6 forum, etc.).

viii Create various customized reports and DUT/EUT test results from testing tools as required and specified by purchaser from time to time.

ix The supplier shall provide assistance in integrating testing tools of the SECURITY TEST lab, including API support, with other labs in purchaser premises and to resolve any problems that may arise during integrated testing of an EUT/DUT.

x The SUPPLIER shall be solely responsible for the maintenance, repair & upgradation of the software/hardware systems, equipment's and parts thereof and purchaser shall not be liable to interact with any of its partners or OEMs.

xi The supplier shall provide assistance including documentary support required for accreditation of lab and its renewal as per the requirements of accreditation agency.

xii SUPPLIER shall provide to purchaser within one week, as part of SUPPLIER's monthly performance reports, a set of reports to verify SUPPLIER's performance and compliance with the Service Levels in a form and structure as approved by the purchaser.

xiii No post-reporting adjustment shall be made to any Service Level performance data or supporting information without purchaser's approval.

12.0 Warranty and Service Level Agreement (SLA):

12.1 The supplied solution shall be under **warranty for a period of two years** from the date of commissioning of the project. The contractor shall provide efficient after-sales support for repair, required Professionals as per clause 5.4 of this section, updates and upgrades of the supplied item(s) in the warranty period and in form of SLA as specified in Clause 11. No separate SLA agreement will be signed as the same will be part of the Purchase Order itself.

12.2 During warranty and acceptance testing the Supplier shall perform all the functions as enunciated under the SLA free of cost. All the penalty and LD clauses shall be applicable during the period of warranty and acceptance testing also in case of failure on part of supplier.

12.3 The supplier shall, undertake to maintain the equipment for hardware, software, firmware and any other related item(s) supplied by them and take full responsibility for their continuous working. The SLA shall include periodic testing, preventive and corrective maintenance including replacement of spare parts. The offered rate for 5 years shall be clearly specified. Supplier shall be responsible for complete technical/operation support during the warranty/SLA period.

12.4 The supplier shall provide necessary technical support including proper documentation and parallel test report of accredited lab using the respective test tool so that the purchaser is able to get the SECURITY TEST lab accredited as per requirement by DOT or any other agency authorized by DOT.

Failure to submit documents and parallel test report for lab accreditation within 6 months after such request from purchaser, due to reasons attributable to supplier shall result in:

(a) Extension of the warranty/SLA of respective tool during warranty period.

(b) Extension of SLA of respective tool and accordingly payment of SLA of that quarter shall be made on completion of extended SLA of that quarter during SLA period

In case of extension of warranty/SLA, the PBG shall also be extended by the supplier, accordingly.

13.0 Evaluation of SLA in Bid:

13.1 The supplier shall quote for Annual Maintenance Service Level Agreement for 5 years beyond 2 year warranty. The cost shall be quoted as a lump sum for maintenance, Updates, Upgradation and visit of the engineers as and when required. The supplier of penetration testing tool and Security Testing Tool for application (SAST & DAST) shall separately quote for the SLA charges for services of professionals for 5 years.

13.2 The evaluation and comparison of responsive bids shall be done on the total price of the respective tool, SLA charges for Annual Maintenance and upgradation and SLA charges for services of professionals (wherever applicable) offered inclusive of Levies & Taxes i.e., GST, packing, forwarding, freight and insurance etc. as indicated in the Price Schedule.

14.0 LIQUIDATED DAMAGES:

14.1 In case testing tool(s) and lab infrastructure item(s) are completely or partially non-available then the severity level shall be defined as per the system non-availability calculated over a period of one month with respect to availability prescribed in clause 19.2. The LD in such cases shall be imposed as:

0.2% of the pro-rata monthly SLA charge (excluding Cost of Services of Professional(s)) for every 0.1% drop in availability. However for the 1st year of warranty the LD shall be 0.2% of the pro-rata monthly SLA charge for every 1% drop in availability. Any drop in availability shall be counted in steps of 0.1% or 1.0% as applicable.

14.2 Delays other than specified above including attending to the dockets, the supplier shall be liable to pay liquidated damages of Rs. 1000 per day which will be deducted from the payments of SLA charges due to the supplier.

14.3 For the liquidated damages accrued during the warranty period, the deduction shall be made from the pending bills for supply of equipment and if required from PBG against the supply contract. The remaining amount, if any, shall be adjusted in the SLA bills/PBG.

14.4 The liquidated damages for carried over faults and upgradation at the end of a quarter of SLA shall be taken in to account while paying the charges for the next quarter of SLA. The LD for carried over faults at the end of SLA shall be taken in to account while paying the charges of last quarter of last year of SLA and if required shall be deducted from PBG.

14.5 Delay in return of repaired card/system, LD charges shall be Rs. 500/day.

14.6 The supplier of penetration testing tool and Security Testing Tool for application (SAST & DAST) must ensure the availability of trained Professional(s) on daily basis. Non availability of Professional(s) will result in LD of 2% per working day of the pro rata monthly cost of services of professional(s), in addition to the pro-rata cost deduction of that day. The per day charge will be calculated by dividing the pro rata monthly cost of services of professional(s) with the no. of working days in the month.

14.7 Delay in replacement of professional(s) beyond two weeks from the request made by the purchaser, LD charges shall be Rs. 2000/day.

14.8 Any delay in the restoration of a fault, as recorded in the FAULT-DOCKET, outside the domain of system availability and system performance, beyond a period of 48 hours, LD charge shall be at Rs 1000/day.

14.9 Liquidated Damages (L/D) shall be recovered from Contract Performance Bank Guarantee (PBG), if the amount to be recovered cannot be adjusted against SLA amount due for the corresponding period. In such a case the Contractor shall replenish the PBG to original value within 30 days of recovery. The PBG shall be renewed from time-to-time till all the liabilities under the contract are resolved by the contractor, or till 6 months beyond the expiry of SLA period of supply, whichever is later.

14.10 Annual Amount of liquidated damages on all accounts during SLA period shall not exceed 1.5 % of total cost of security testing tools. This limit also applies to LD charges as mentioned in clause 9.3 and clause 10.8 of Section IV.

15.0 Annual Maintenance SLA CHARGES AND PAYMENTS:

15.1 The charges for SLA will be as given in the purchase order.

15.2 Purchaser shall not pay any charges in advance.

15.3 The payment for SLA, after completion of warranty, shall be made quarterly on pro rata basis based on production of bill/invoice duly certified by Purchaser representative for successful execution of SLA. The payment will normally be released within 30 (thirty) days of the receipt of the bill duly completed and endorsed by the SECURITY TEST Lab in-charge.

15.4 Payments shall be made after deducting LD if any and statutory levies and taxes.

15.5 Purchaser reserves the right to adjust any over-payment of SLA charges, any time during the period of SLA.

15.6 If the fault occurs at the end of an SLA period of any quarter it will be carried forward to the next SLA period of next quarter.

15.7 The faults/complaints reported before completion of last year of SLA and remaining unattended/unrectified will have to be rectified without any payment after completion of SLA contract of 5 Years.

16.0 MAINTENANCE OF HISTORY SHEET AND LOG BOOKS:

16.1 The designated in-charge of the SECURITY TEST Lab shall maintain a log book/ history sheet to record, events including alarm, faults (including restarts) and updates and upgrade activities, test in progress etc., which shall be verified by supplier.

16.2 History sheet proforma shall become part of this agreement. Purchaser reserves the right to make changes in the proforma proposed by the Supplier which shall be submitted at the time of installation.

16.3 The Supplier shall provide detailed maintenance procedures and proforma of the history sheet. The officer In charge of the Security Test Lab shall fill up the history sheet containing the statistics about the health of the Security Test Lab equipments installed at the Lab and send a report to the Technical support and national Center of the Supplier on monthly basis. Based on the History sheet report, the Supplier shall analyze the health record of Security Test Lab and if something alarming or unusual is noticed, shall advise the in-charge of Security Test Lab to take necessary actions for preventive maintenance of such equipments. These instructions for preventive maintenance shall be passed on to Security Test Lab staff in writing and by sending experts to the SECURITY TEST lab as special activity.

17.0 Software License:

All software prices shall be quoted on fixed price basis including license fee for the entire contract period.

18.0 List of Essential Spares:

Sufficient number of replaceable spare parts shall be kept by the supplier at the purchaser premises. The SLA quote shall be with user replaceable spares stocked by supplier at his cost at the purchaser premises. The list of spares, if applicable, should be submitted at the time of acceptance testing.

19.0 INCIDENT MANAGEMENT - HARDWARE AND SOFTWARE DEFECT:

19.1 Following Hardware and Software defects shall be treated as non-availability:

(a) Testing tool crash or complete disruption of testing activities.

(b) Any performance degradation which means testing tool hangs (stuck) - testing tool not operative, or there is unreasonable wait times for resources or response as if the testing tool is hanging

(c) Testing tool crashes repeatedly under normal use.

(d) Operational error which means testing tool is impaired in full or in part.

19.2 Permissible Minimum Availability of Security Lab tools

System availability	Metric (Uptime)
Vulnerability Assessment Tools (CVE and CCS7)	99 %
Fuzzing Tool (Ethernet Interface)	99%
Static code Analysis and Dynamic Analysis Application Security Testing Tool)	99 %
Binary Analysis tool	99 %
Penetration testing tool	99 %

i. The metric values of the availability of the lab tools are inclusive of any planned outages and are measured over a period of one month.

ii. The desired system availability over a defined period shall be ensured. Scheduled backup and other recovery functions must be clearly identified by the supplier.

iii. In case a testing tool is completely or partially not-available then the severity level shall be defined as per the testing tool non-availability calculated over a period of one month. The LD in such cases shall be imposed as per clause 14 of Section IV.

19.3 TECHNICAL SUPPORT CENTRE:

i) The supplier shall have at least one Technical Support Center in India. The supplier may decide the location, resources, manpower, etc. of such Center so as to meet the criteria for fault restoration/faulty unit repair times as mentioned in the SLA. The SUPPLIER shall furnish the names, locations, complete postal address, Email address, Telephone numbers and FAX numbers of the Technical Support Center at the time of signing this

Agreement. The SUPPLIER shall also specify the details of Technical Support Center in the format given below.

Details of Technical Support Center

1. Location of Technical Support Center:
2. Name of the Contact person:
3. Postal Address:
4. Telephone Numbers Minimum two:
5. Mobile Phone Number:
6. FAX Number:
7. e-mail:

ii) The SUPPLIER shall also provide the name of alternate contact person or Technical Support Center with address/ email address & telephone /FAX no. which may be contacted by purchaser staff for support in case of no response/poor response from the designated Technical support center. This, however, shall not preclude purchaser from imposing the penalties, if any, as applicable as per the terms & conditions of this agreement.

iii) Any change in Address, Email address, Phone number, FAX Number etc shall have to be intimated in writing by the SUPPLIER to the concerned In charge of the Security test lab at the earliest. If the station In charge of the Security test lab is unable to report the faults to the normally assigned Technical support Center due to the change of email, phone number etc. the fault will be reported (as per provision of (i) above) and the SUPPLIER shall be responsible for rendering all the maintenance support services to the SECURITY TEST lab as per the terms and conditions of this Agreement.

20.0 RESPONSIBILITIES OF TECHNICAL SUPPORT CENTER:

20.1 The SUPPLIER shall ensure that the Technical support center(s) is/are manned by fully competent and responsible Engineers, who are:

a) Capable of giving all types of necessary technical guidance/ assistance over phone to the In-charge of Security test lab, for fast restoration of faults. Telephonic assistance shall be made available between 9am to 6 pm IST from Monday to Saturday.

b) Capable of attending the faults in testing tool(s) and lab infrastructure item(s) at the Security test lab site whenever needed by deputing competent technical expert.

20.2 The other responsibilities of the supplier for their respective tool(s) and lab infrastructure item(s) are:

i) The Technical support Center shall collect the faulty modules/cards/units/PCBs etc. from Security test lab and repair / replace them with good cards during the period of SLA.

ii) The SUPPLIER shall either carry-out the repair on its own or through the facilities of third party or parent company. In all cases, however, purchaser shall interface only with this SUPPLIER.

iii) The first line maintenance shall be done by authorized staff of supplier by replacement of the faulty /affected Hardware/ Software module with a readily available good Hardware/ software module, stocked at the site by the SUPPLIER at his (Supplier's) cost or out of the spare capacity or any other module arranged by the supplier as the case may be. Decision whether the Hardware/ Software module / cards for the respective tools and lab infrastructure item(s) at SECURITY TEST Lab can be made spare or not shall rest with purchaser.

iv) The responsibility of packing & dispatch of faulty Hardware/ Software modules/ cards/ units/ PCB etc. at the site of purchaser as well as at the repair/ maintenance site shall lie with the Supplier.

v) The SUPPLIER shall ensure repair or replacement of the faulty equipment/card, within 30 days (including transit time) of reporting of the faulty equipment from purchaser to the SUPPLIER's designated Technical support Centre. The cost of transport on both sides shall be borne by the SUPPLIER. The 30 days' time shall be calculated from the date of reporting the faulty equipment at the SUPPLIER's designated premises to the date of receiving back of the repaired / replacement of the same at purchaser.

vi) The Supplier shall set up Fault Management System to register the fault dockets and its management.

21.0 TECHNICAL SUPPORT PROCEDURE:

21.1 The following procedure shall be followed for Technical support:

i) In case of any fault, abnormality in the system, partial or total failure of the system, the officer In-charge of the Security test lab will immediately contact the designated Technical support Center of the SUPPLIER and give information about the nature of fault over phone / FAX /e-mail.

ii) The details of the faults reported shall be recorded in a prescribed format, called the **"FAULT – DOCKET"** as given in **Appendix-A** of this Agreement. Changes in the "FAULT – DOCKET" may be incorporated for better reporting and recording reconciliation of the faults at Security test lab and also at Technical Support Center of the SUPPLIER by mutual agreement and understanding, to best utilize the Fault Docket facility as and when such need is felt. To this end changes in fault reporting procedures can also be incorporated.

iii) Even if the fault is reported over phone to the Technical Support Center a copy of the "Fault Docket" duly filled in by the officer In-charge of Security test lab shall be sent by FAX/email to the Technical support Center of the SUPPLIER for records. The time of occurrence of fault as recorded in the fault docket shall only be taken into consideration for calculating the actual duration of faults.

iv) Similarly, after rectification of fault a fresh Fault- Docket duly filled in and after recording the time of restoration and total duration of fault, will be sent by officer In-charge of Security test lab to the Technical support Center, preferably by FAX/email, for records.

v) In case of any dispute arising regarding duration of fault etc., the Fault Docket as maintained at the Security test lab station shall be the guiding documents to be agreed by both parties.

vi) The "Fault Docket" shall be filled with utmost care, giving all the details of the faults and other information as prescribed in the Fault Docket and the entries made shall be authenticated by signature of the station In-charge of the Security test lab.

vii) Technical instructions shall be given to the Security test lab staff over phone. If the fault is restored by following the instructions given over phone, the officer In charge of Security test lab will close the Fault Docket after making suitable entries and after satisfying himself/herself of the proper restoration of the fault. A copy of the Fault Docket duly filled in shall be sent to the Technical support Center for records.

viii) The SUPPLIER shall also ensure visits of the expert and competent technical staff of the SUPPLIER in case the fault is not rectified to the satisfaction of the purchaser even after following the telephonic instructions and advices.

ix) Once the fault has been rectified and the system & services were restored to normalcy, the visiting engineer of the SUPPLIER shall record in the **station Log Book**, the details of the works done by him for restoration of the faults. Similar entries shall be made in the fault docket also.

x) Any delay in the restoration of a fault, as recorded in the **FAULT-DOCKET,** which comes in the domain of system availability and system performance shall be penalized in accordance to clause 14 of this Section.

Stamp and signature of bidder

Appendix-A to the SLA

TELECOM ENGINEERING CENTRE
FAULT- DOCKET FOR SECURITY TEST LAB

Docket Sl. No:
File No: Date:
From:-
Name:
(of the officer in-charge/duty officer of the Lab)
Designation:
To,
M/s.---------- (the SUPPLIER)
Address:
(of the Technical support / Center)

1. 1. Date ---------- Time---------- (of occurrence of fault)

1.2. Date.---------- Time---------- (of Reporting of Fault)
2. Fault Reported to: Technical support Center (Name of the person) on phone :

3.1 Mode of Reporting : Phone/SMS/FAX/Email/……
(Tick whichever is applicable)

3.2 Fault observed in(Testing tool(s)/Lab infrastructure item(s)):----------
(Tick whichever is applicable)

4. Description of fault & observation of the reporting officer:

5. Details of Services affected :
6. Percentage of Service affected :

7. Date_____ Time _____ (of receiving the 1st assistance over phone from Technical support Center)

8. Details of Assistance received :
(Note: Add additional sheet if needed.)

9. Date_____ Time _____ (of receiving the 2nd assistance over phone from Technical support Center)

10. Details of assistance received :

Stamp and signature of bidder

(Note: Add additional sheet if needed.)

11. Was the fault restored by following the instructions given over phone ?

A- YES ☐ B- NO☐ (Tick whichever is applicable)

12. If Yes, record date & time of restoration & duration of fault :

Date_____ Time _____(in hours & minutes)

Duration of Fault: _____ days _____ Hours _____minutes.

13. Was the fault restored:

A- Partially B- Fully (Tick whichever is applicable)

14. If the fault is not restored or restored only partially, give details of observation:

(Note: Add additional sheet if needed)

15. Note date & time of giving feed back vide Srl No:14 above to the Technical support Center:

(only in the event of partial / non restoration of faults)

Date _____ Time _____ . (in hours & minutes)

16. Date & Time of arrival of SUPPLIER's Expert at site / station of fault :

Date _____ Time _____ . (in hours & minutes)

17. Brief observation and works done by the SUPPLIER's staff / expert :

(detailed entry to be made by SUPPLIER's staff in the station Log-Book)

18. Date & Time of complete restoration of the system :

Date _____ Time _____ . (in hours & minutes)

19. Total Duration of Fault : _____ days _____ hrs _____minutes.

20. Remarks of Officer In charge (if any) :

21. Remarks of visiting engineer (of SUPPLIER), if any :

Signature :
Name :
Designation :
(of TEC staff / In charge of the SECURITY TEST LAB)

Note:

1 Each page of the Docket must be signed by designated officer of TEC(including the additional sheets, if attached)
2 A copy of the Fault- Docket must be sent to the Technical support Center of the SUPPLIER, immediately by FAX / Post after restoration of fault.
3 At the time of first reporting it may not be possible to pinpoint the fault. Hence more than one boxes can be ticked against Sl.3.2 . Similarly observation of the local impact of fault may not be possible against Sl.5. The duty officer shall provide observation which are immediately available.
4 Date on percentage of services affected shall be made available by the supplier though Root Cause Analysis as provided under special conditions.

Stamp and signature of bidder

SECTION - V
TECHNICAL SPECIFICATIONS & SCHEDULE OF REQUIREMENT

A. TECHNICAL SPECIFICATIONS:

1. Objective & Scope:

a. Objective:

The objective of this test lab is:

i. Proactive detection of vulnerabilities in elements of deployable or deployed telecom systems and/or networks before the vulnerabilities are exploited. This includes identification, understanding and verification of weaknesses, misconfigurations and vulnerabilities within all types of end user devices and nodes in a telecom network.
ii. To find security bugs / malwares in server/client application softwares.
iii. To test the resiliency of a DUT (device under test e.g. network nodes and CPEs) against vulnerabilities related to Distributed denial of service (DDoS) attacks, Botnets, Phishing, identity theft, Advanced Persistent Threats etc.

b. Scope:

The scope of this tender is to set up Telecom security Test (SECURITY TEST) lab with the Security testing tools capable of testing the security features of all types of IP and telecom / ICT equipment in access, transport, control and application layers of wireless and wire line domain deployed and likely to be deployed in the telecom network e.g. NGN, IMS, LTE and M2M etc. and various types of End User Devices such as mobile handsets, dongles, tablets, modems etc. and CPE devices such as Residential Gateways, LTE- CPE devices with Wi-Fi interfaces towards user etc. The Security testing tools should comply to the international security testing standards and test schedules prescribed by CC / ITU-T/ ETSI / 3GPP/IEEE/ 3GPP2 wherever applicable as well as those prescribed by DoT or any other agency authorized by DoT within the scope of ordered tender item(s).

For the purpose of this tender the category of tests can be broadly divided in, but not limited to, the following five groups:

i. Vulnerability assessment tool for detection of known vulnerabilities
ii. Fuzz testing tool for detection of unknown vulnerabilities
iii. Static Code analysis Tool and Dynamic Application Security testing tool
iv. Binary analysis tool
v. Penetration testing tool for exploiting the detected vulnerabilities.

The scope of tender shall also include generation of a final test report in a standard format (e.g. pdf and html) from various tools and providing mitigation recommendations.

2. Requirements for the Testing tools for security testing:

All the tools supplied shall be of commercial or professional version with perpetual license. The requirements of the various tools used in the security test lab shall be as follows:

2.1 Vulnerability assessment tool:

i. There shall be 2 types of Vulnerability assessment tools, One CVE compliant and other for CCS-7 related testing.

ii. Vulnerability assessment tool supplied shall be capable of scanning targets i.e. network nodes including end user devices, the operating systems, databases, and/or Web applications residing on those nodes in an attempt to detect known vulnerabilities.

iii. The identified vulnerabilities shall comply to latest CVE catalogue as well as any other telecom vulnerabilities in access network, core network and end user devices including any other prevalent standard at the time of placement of purchase order as per standard catalogue available publicly and commercially.

iv. The supplied Vulnerability assessment tool shall be capable of doing the scanning of individual devices connected to the tool on one to one basis and / or a range of devices connected to the tool through LAN as well as WAN network.

v. The supplied tool shall begin its assessment by performing a "footprint" analysis that involves first discovering all open ports on a device under test, then scanning these ports to enumerate all of the available services on the device to determine which services and/or software programs (including versions and patch levels) are running on the target. The tool shall also have the capability of assessing by "footprint" analysis of first discovering all active nodes on the network, then scanning them to enumerate all of the available network services on each host to determine which network services and/or software programs (including versions and patch levels) are running on the target. Then the supplied tool shall attempt to identify (patterns/ attributes of) the known vulnerabilities, in the detected services/software versions, and then report their findings as result.

vi. Active scanning i.e. scanning followed by validation of the detected vulnerabilities shall be performed by the supplied tool to verify that those vulnerabilities are, in fact, both present as well as exploitable. The tool shall be capable of analyzing false positives i.e., the instances in which the scanner detects a pattern or attribute indicative of a likely vulnerability, which upon further analysis proves to be either not present or not exploitable.

vii. The supplied Vulnerability Assessment tools shall be capable of scanning a number of network nodes, both local and remote, including networking and

networked devices (Mobiles, Modems, set top box etc. switches, routers, firewalls, printers, etc.), as well as server, desktop, and portable computers.

viii. The tool shall be able to schedule scans at specific starting dates and time, frequencies and maximum scan durations.

ix. The tool shall be able to automatically pause scheduled scans if unable to complete within the predefined durations.

x. Each purchased single user license of the tool shall support testing of at least 20 devices/IP simultaneously.

xi. The tool shall be upgrade the IP license to a larger in case need to scan more IPs.

xii. The tool shall be able to support both credentialed and non-credentialed scans which include but is not limited to: SNMP, SSH, WINDOWS.

xiii. The tool shall run on Windows, Linux (all distributions) OS operating environment.

xiv. The tool must support the automatic discovery of virtual assets on VMware

xv. The tool must support integration with IDS/IPS products.

xvi. The reports generated by the supplied vulnerability assessment tool shall also provide categorization/prioritization, exact remediation for individual vulnerabilities, and recommendations on how to fix and improve the security of the DUT / EUT and overall network in line with the best practices.

xvii. The tool shall be able to integrate native exploit information from well-known sources, minimally with ExploitDB and Metasploit database.

xviii. The tool shall support integration with external penetration testing platforms to perform and automatic vulnerabilities exploitation.

xix. The tool shall be able to identify known exploits and malware kits associated with detected vulnerabilities.

xx. There shall not be any need to load or maintain any client software on the targets i.e. device under test.

xxi. The vulnerability knowledge database for this tool shall comprise of all the published vulnerabilities as per latest CVE catalogue including any other prevalent standard at the time of placement of purchase order as per standard catalogue available publicly and commercially. The supplier shall

ensure the upgradation of library of known vulnerabilities on a weekly basis in complete synchronization with the vulnerabilities published in the CVE catalogue as well as any other telecom vulnerabilities catalogue.

xxii. The library of the vulnerability assessment tools shall be updated on a regular basis with the most recent security vulnerabilities and shall contain a complete trigger list of all possible known attacks e.g. DDoS, Buffer overflow, SQL injection, eavesdropping, session hijacking, APT, BOTs etc.

xxiii. The tool shall be coded with maximum coverage of plugin's (which is a simple program that checks for a given flaw) covering of local and remote flaws.

xxiv. The tool shall be able to perform both automatic & manual (Plugins/ Software updates).

xxv. The tool shall identify misconfigurations in target device like missing patches in OS/applications etc.

xxvi. The tool shall support integration with Active Directory, Kerberos, or any LDAP compliant directory.

xxvii. The tool shall be with web application scanning solution must support coverage of latest OWASP vulnerabilities.

xxviii. It shall be capable of scanning all the operating systems, firmware, databases, protocols and applications being used by telecom equipment including smartphones, tablets, dongles, modems, all types of wireless access points, routers, switches and perimeter devices e.g. firewalls, IDSs, IPSs, UTMs etc.

xxix. The supplier shall provide suitable on-site mechanism to customize the format of the report generated by the tool as per the requirement of the purchaser.

xxx. The tool shall be upgraded by the supplier with capabilities for scanning new operating systems, firmware, databases, protocols and applications being used by telecom equipment including smartphones, tablets, dongles, modems, all types of wireless access points within 3 months from the date of request by the purchaser.

xxxi. The tool shall provide user friendly interface for testing and report generation.

xxxii. It shall be possible to access the tool and conduct testing lifecycle from the User interface from the desktop client.

xxxiii. It shall be possible to store and transfer the test results to the test result repository server in the network for record keeping.

2.2 Fuzzing tool:

Fuzzing tool, for Ethernet interface (Fuzzer-E)

i. Fuzzer-E shall comply with generation based fuzzing of protocols mentioned in list A and list B of Annexure and. In case CCS7 protocols of List A and List B are not possible to be tested through Ethernet based Fuzzer, then separate tool shall be provided for CCS7 protocols at no extra cost to the purchaser along with Ethernet based Fuzzer.

ii. Fuzzing tool shall be capable of discovering unknown / zero day vulnerabilities in a target by providing unexpected inputs towards it and monitoring the target for exceptional behavior.

iii. It shall be capable of doing *generation-based fuzzing* as well as *mutation-based fuzzing.* Generation-based fuzzing tools create test cases from scratch by modeling the target protocol or file format. Mutation-based fuzzing tool here means that the fuzzing tool, which apply mutations on captured data samples to create test cases.

iv. Fuzzer-E shall be capable of doing the following types of fuzzing in a fully automated manner:

   a Protocol fuzzing for protocols mentioned in Annexure IX being used in telecom network nodes as well as end user devices.
   b Operating system and firmware fuzzing.
   c Application fuzzing for all applications running in client devices (e.g. smart phones) as well as those hosted on servers.
   d Web browser fuzzing to uncover the bugs in web browsers.
   e File format fuzzing to detect the unknown vulnerabilities present in maliciously crafted files for the file formats mentioned in list A and list B of Annexure.

v. Protocol fuzzing done by the supplied tool shall be dynamic and stateful with in-built complete protocol state machines that enable robustness testing deep within the target protocol's software layers and state transitions. It shall support fuzzing throughout every message exchange and transition that a protocol supports in a real operating environment.

vi. All the standard protocols including custom and proprietary extensions shall be supported. Addition of new protocols to this tool in future shall also be supported within six months from the date of request by the purchaser.

vii. Other than detecting the hard crashes, the supplied fuzzing tool shall be capable of detecting and reporting the soft faults e.g. delayed response. Any other capability of detecting and reporting faults shall be listed by the supplier along with the bid.

viii. The supplied fuzzing tool shall also monitor the behaviour of the device under test (DUT), and correlate cause and effect between the specific negative test case(s) and the abnormal behaviour. For every such fault identified, it shall perform automated data collection, alerting and

reporting. It shall enable the user to implement the reproduction of bugs identified. The tool shall support both in-band and out-of-band instrumentation. In-band instrumentation is used to obtain the crash - no crash status and usually consists of sending a valid protocol request to the DUT. The tool shall support both SNMP checks and Syslog checks as out-of-band instrumentation methods used to obtain DUT state information.

ix. Tool shall be capable of identifying the following responses of the DUT to the fuzz testing:
- The DUT crashes and is unable to restart
- The DUT crashes and then possibly restarts.
- The DUT hangs in a busy loop, causing a permanent Denial of Service situation.
- The DUT slows down momentarily causing a temporary Denial-of- Service situation.
- The DUT fails to provide useful services causing a Denial-of-Service situation (i.e. new network connections are refused)

x. It shall be possible for the tester to choose the test cases to be run as per need, based on protocol PDU fields, message type, etc. It shall also be possible for the tester to run the most effective attack patterns for different fields of the protocol to keep the test run time reasonable.

xi. The tool should be capable of checking interoperability between Test tool and DUT for all the protocols mentioned in Annexure A and Annexure B.

xii. The tool should be installable and executable on all popular operating Systems platforms with 32 bit and 64 bit versions (on personal Computers).

xiii. It shall have a user-friendly graphical user interface as well as command line interface for handling and operation of the Fuzzing techniques supported and the analytical abilities provided. A very well documented user manual shall be made available for this purpose.

xiv. The supplier shall ensure that in case of power failure or abrupt shutdown, the Fuzzer tool shall resume the testing from the point at which the shutdown occurred. It should not happen that the tool starts performing the fuzzing from the beginning unless required by the user / purchaser.

xv. The generated reports shall also provide prioritization of the detected vulnerabilities highlighting the most critical problems first. It shall be able to capture critical details from the DUT during the fault event or crash, and provide actionable remedies along with packet captures (PCAPs) and External Vulnerability Triggers / exploits.

xvi. The tools shall maintain a detailed log of the fuzz testing and it shall be possible for the tester to access the log details at any time. It shall be possible to export the log file to an external storage in standard file formats that will enable viewing of the test information at any point of time.

Stamp and signature of bidder

xvii. A single license of Fuzzer shall provide simultaneous testing of atleast 20 devices, of all the protocols, file formats, operating system, firmware, web browser.

xviii. All the file formats and protocols mentioned in Protocol List A for the Fuzzer E of the Annexure, shall be essentially supported at the time of submission of bid. However, the Supplier shall be required to comply with List B (as applicable) of Annexure within 365 days from date of placement of PO.

In case a DUT offered in SECURITY TEST Lab requires testing of any file formats and protocols mentioned in List B for Fuzzer-E, purchaser reserves the right to demand support for one or more protocols mentioned therein. The supplier shall have to comply this within three months from the date of request by the purchaser.

xix. The supplier shall provide a suitable on-site mechanism to customize the format of the report generated by the tool as per the requirement of the purchaser.

xx. The supplied tool shall be upgraded by the supplier for the latest telecom protocols in access, transport, control and application layers of wireless and wire line domain including 4G and 5G protocols during the entire contract period.

xxi. For the remaining protocols, the supplied tool shall be upgradable and supplier shall provide the required tools/SDK for development of generation based fuzzing for telecom protocols defined in ITU-T,3GPP, IETF etc. and generation/mutation based fuzzing for all the custom and proprietary extensions and mutation based fuzzing for any identified protocols as per request made by purchaser.

xxii. It shall be possible to access the tool and conduct testing lifecycle from the User interface from the desktop client.

xxiii. It shall be possible to store and transfer the test results to the test result repository server in the network for record keeping.

2.3 Static Code Analysis Tool and Dynamic Application Security Testing Tool (DAST):

The supplier shall provide both static and dynamic analysis security testing capability either through same tool or separate tool at no extra cost to the purchaser.

2.3.1 Static Code Analysis Tool:

i. The supplied tool shall be capable of automatically scanning source code of any type to identify the exact locations of security vulnerabilities that can be

exploited. It shall scan the source code vulnerabilities against all the prevalent security coding vulnerability databases (e.g. CWE, SANS TOP 25, OWASP TOP 10, CVE)

ii. It shall correlate and prioritize results to deliver an accurate, risk-ranked list of issue along with corresponding CWE code to ensure that the most serious issues are addressed first. It shall provide detailed guidance on how to fix the vulnerabilities at the line-of-code level.

iii. It shall be a platform independent tool and support variety of operating systems such as Windows, Linux, MacOS and should allow scanning of different coding languages used in software/firmware of telecom/ICT products, CPEs, mobile phones, applications etc. without installing and updating the respective compilers.

iv. The supplied tool shall be capable of checking the source code compliance as per the secure coding standards e.g. Cert C, Cert Java, Cert C++, CWE Database, ISO/IEC TS 17961 and any other coding standards prevalent on the date of placement of purchase order of this tool covering the devices mentioned in clause 2.3.1(iii). In addition to this, it shall be possible to customize the tool for a user defined coding standard i.e. the standards adapted by the manufacturers of the DUTs.

v. It shall be capable of detecting malicious code insertion, which may result into exploitation of array bound overflow and buffer overflow.

vi. It shall have a user-friendly graphical user interface for all programming languages. A web based GUI along with CLI is preferred.

vii. The tool shall generate reports like:

a. Summary reports (e.g.: Vulnerability category wise reports (memory leaks, API abuse, buffer overflow and so on), Severity wise reports, Configuration reports)

b. Technical Detailed Report providing all the details of the identified vulnerabilities like category of the Vulnerability, CWE code, Location of the Vulnerability including file name and line number of code, Remediation advice along with code samples in the same programming language and so on.

viii. The tool shall capable of generating the report in standard format and supplier shall provide a suitable on-site mechanism to customize the format of the report generated by the tool as per the requirement of the purchaser.

ix. The supplied tool shall be updated and upgraded with new versions of all the coding languages supported by the tool during the entire period of contract.

x. The supplied tool shall also be upgraded with new coding languages/ scripts/ structures etc. used in the telecom or IT software/ firmware domain within 3 months from the date of request by the purchaser.

xi. It shall provide compliance against any new/ modified international coding standards within 3 months from the date of request by the purchaser.

xii. It shall be updated to provide compliance for all the new additions in OWASP, SANS and CWE standards of coding weaknesses within a 15 days' time frame from the date of release of such additions.

xiii. It shall be capable to identify Control flow, Pattern/rule based analysis and Data flow anomalies like Un-initialized variables, defined but unused variables, defined then defined again without being used, etc.
xiv. It shall be capable to do Information Flow analysis to identify inter dependencies of programming variables like strong/ weak dependencies, Direct/ Indirect dependencies and Conditional/Unconditional dependencies.
xv. It shall be capable to do structural coverage analysis to measure what code has been executed
xvi. The tool shall have an acceptably low false positive rate.
xvii. It shall be possible to access the tool and conduct testing lifecycle from the User interface from the desktop client.
xviii. It shall be possible to store and transfer the test results to the test result repository server in the network for record keeping
xix. There shall not be any limit to number of lines of code that the tool shall review.
xx. The single license of tool shall be able to support testing of atleast 20 devices simultaneously.

2.3.2 Dynamic Application Security Testing tool:

i. The tool shall support security testing of mobile and web applications on different platforms.
ii. The tool shall support security testing of web services.
iii. The tool shall able to compare and report two different scans to enable a delta analysis which also includes the representation of vulnerability difference between two scans.
iv. The tool shall have the capability of performing vulnerability checks and tests as per OWASP top 10 related vulnerabilities.
v. It shall be capable to do dynamic analysis to measure statement coverage to ensure maximum coverage and having less bugs for higher assurance
vi. It shall be capable to do dynamic analysis to measure function coverage to ensure all functions in a software programme are invoked (executed)
vii. It shall be capable to do dynamic analysis to measure coverage to ensure that all branches/ control in a software programme are invoked.
viii. It shall be capable to do dynamic analysis at system testing level (completed programme), Module level (files contains many functions) and Unit level (files contains single function)
ix. It shall be capable of generating dynamic flow graphs to view system level coverage, Module level coverage and Function level coverage
x. It shall be possible to access the tool and conduct testing lifecycle from the User interface from the desktop client.
xi. It shall be possible to store and transfer the test results to the test result repository server in the network for record keeping.
xii. The single license of tool shall be able to support testing of atleast 20 devices simultaneously.

Stamp and signature of bidder

2.4 Binary Analysis tool:

i. This tool shall be capable of evaluating vulnerabilities introduced by linked libraries, APIs, web services compiler optimizations and third party components by looking at the code in its "final" compiled version.

ii. The supplied binary analysis tool shall be capable of detecting threats introduced as a result of malicious codes and backdoors by analyzing all code paths and data flows that the program will execute.

iii. It shall also examine communication among components for any weaknesses introduced during linkage.

iv. The tool shall provide reports in standard format. The generated report shall help in fixing the most severe vulnerabilities first and should point out the exact location of code creating each problem. It shall also provide supplementary details about the nature of the issue and recommend a specific fix.

v. The tool shall be platform independent and shall have a user friendly web based GUI. It shall also support all processing architectures prevailing at the time of supply

vi. It shall be updated and upgraded by the supplier for supporting the new coding languages, libraries, APIs, compiler optimizations, executable file versions and third party components used in the telecom or IT software / firmware domain including CPEs, mobile phones, applications etc. within a time frame of 3 months from the date of request by the purchaser during the entire period of contract.

vii. The supplier shall upgrade the tool's capabilities for scanning the executables related to new operating systems, firmware, databases, protocols and applications being used by telecom equipment, smartphones, tablets, dongles, modems, all types of wireless access points etc. within 3 months from date of request by the purchaser during the entire period of contract.

viii. The supplier shall upgrade the tool's capabilities for scanning the executables related to upgraded versions of existing operating systems, firmware, databases, protocols and applications etc. already supported by the tool within 3 months of their release during the entire period of contract.

ix. It shall be updated by the supplier for detection of new threats as per the weaknesses included in the OWASP, SANS, CWE lists etc. within a 15 days' time frame from the date of release of such additions.

x. It shall report for the extra executable or files which are not the part of the software release offered.

xi. The supplier shall provide a suitable on-site mechanism to customize the format of the report generated by the tool as per the requirement of the purchaser.

xii. It shall be possible to access the tool and conduct testing lifecycle from the User interface from the desktop client.

xiii. It shall be possible to store and transfer the test results to the test result repository server in the network for record keeping.

xiv. The single license of tool shall be able to support testing of atleast 20 devices simultaneously.

2.5 Penetration testing tool:

i. Penetration testing tool shall be capable of launching attacks on targets /systems under test for exploiting the detected vulnerabilities.

ii. It shall determine whether the detected vulnerabilities are actually exploitable.

iii. This tool shall correlate and prioritize results to deliver an accurate, risk-ranked list of issue to ensure that the most serious issues are addressed first. It shall generate actionable data in the form of detailed reports highlighting risks of targeted systems, tests conducted, vulnerabilities exploited, and attack paths followed plus links to patches for the detected vulnerabilities and other remediation data.

iv. It shall have the capabilities of addressing a wide range of threat vectors related to various types of networks, operating systems, Desktop applications, Web applications, server, databases and end user devices.

v. It shall also have the capability of development of new customized exploits, as well as augmentation or modifications in the existing exploits. These customizations or modifications shall be possible without any expertise in programming languages.

vi. The tool shall be platform independent and shall have a user friendly web based GUI.

vii. The supplier shall provide a suitable on-site mechanism to customize the format of the report generated by the tool as per the requirement of the purchaser.

viii. The tool shall support importing of scan result from external tools including but not limited to Nexpose, NetSparker, Nessus, Burpsuite, Acunetix, AppScan etc.

ix. The tool shall support brute force testing on services including but not limited to DB2, MySQL, MSSQL, HTTP, HTTPS, SSH, Telnet, FTP, POP3, SNMP.

x. The tool shall support web crawling on IPv4 and IPv6 web sites.
xi. The tool shall support detection of vulnerable URLs as per latest OWASP TOP10 standards.
xii. The tool shall support web crawling a minimum of 4 Websites concurrently
xiii. The supplier shall update its library of exploits on a continuous basis as per the CVE catalogue updation at least once in a week. All the exploits must be thoroughly tested prior to its incorporation in the SECURITY TEST lab.
xiv. The supplier shall continually update and upgrade its manual exploit development and customization module, on its own, as per the latest techniques and best practices available in the market, but not later than 3 months from the date of request made by the purchaser.
xv. It shall be possible to access the tool and conduct testing lifecycle from the User interface from the desktop client.
xvi. It shall be possible to store and transfer the test results to the test result repository server in the network for record keeping.
xvii. The single license of tool shall be able to support testing of atleast 20 devices simultaneously.

3. Other Technical Requirements:

The requirements mentioned in this clause are requirements applicable to testing tools, in general.

i. **In-house installed solution**: All the tools supplied for the lab shall be installed in TEC lab premises. None of the solution shall be cloud based.

ii. **Lab set-up:** Indicative Lab setup is given in Figure-1. The dimensioning of the tool hardware shall be such that the performance of the tools shall not be degraded during the entire period of contract. If at any stage a degradation is observed, the supplier shall have to supply additional hardware or upgrade the existing hardware. Additionally, augmentation of server (including power supply), at no extra cost to the purchaser, shall be due in case the processor or memory occupancy touches 60% while handing simultaneous testing of multiple DUTs as envisaged in the project.

iii. **Operating System / Platform:** The tools in the lab shall be based on standard operating systems of Windows or Unix (FreeBSD or variants)/ Linux.

iv. All equipment's shall be IPv6 complied.

v. **A.C. power supply:** A.C. power supply shall be made available by the purchaser in the lab. All the tools and devices such as routers, LAN switch, server shall work on A.C. supply. The server hardware for the tools shall preferably be Rack mountable. Purchaser shall provide standard 42U rack with installation of tools in Security Lab.

vi. **Adapters:** All the testing tools and lab infrastructure items shall be supplied along with necessary adapters/accessories to facilitate connectivity, interfacing and testing of various DUTs. All the optical interfaces and electrical interfaces shall be supplied along with cables/patch cords of at least 20m length. Attenuators for all the optical interfaces on the tool shall be supplied.

vii. **Accreditation:** The testing tool supplier shall be responsible for support related to all documentation, certification etc. required for accreditation as specified by DoT.

4. SLA/Warranty:

SLA/ Warranty shall be as per section IV.

5. Software & hardware upgrades requirements:

i. There shall be no need to upgrade the software when the hardware port(s) is/are added in the lab equipment.

ii. The supplier shall undertake to supply on continuing basis all software updates free of cost, for a period of seven years (Warranty plus SLA) from the date of taking over of lab. These updates shall include new features and services and other maintenance updates. The supplier shall quote SLA cost for 5 years.

iii. Direct download of updates and upgrades on lab equipment shall not be permitted. It shall first be downloaded on a separate workstation dedicated for this purpose, sanitized for the presence of any virus, malware etc. and then it shall be loaded on the actual lab equipment.

iv. The supplier and/or its OEMs shall have the facilities for software maintenance like software debugging, patch development, patch verification, patch implementation at sites, version control of software, document generation and repository of working versions.

6. EMC/EMI, Quality & Environmental Requirements:

6.1 EMI/EMC Requirements

The routers, LAN switches, Firewall, Server and testing tools shall confirm to EMI/EMC requirements as per TEC Standard no. TEC/SD/DD/EMC-221/05/OCT-16

6.2 Safety Requirements

(i) The operating personnel should be protected against shock hazards as per IS 8437 {1993} "Guide on the effects of current passing through the human body" [equivalent to IEC publication 60479-1{2005}].

(ii) The equipment shall conform to IS 13252-1 {2010} "Safety of information technology equipment including electrical business equipment" [equivalent to IEC publication 60950-1 {2005} *with amendment 1 (2009) & amendment 2 (2013)*] and IS 10437 {1986} "Safety requirements of radio transmitting equipments" [equivalent to IEC publication 60215(1987)].

6.3 Environmental requirements:

i. The system shall be able to work satisfactorily over the temperature range of 0 - 45 degree Celsius.

ii. The system shall be able to work satisfactorily over the Humidity range of 8% to 80%

7. Minimum Requirement for domain expert professionals for Application Security testing tool and Penetration testing tool:

A. **Domain Expert Professional for Security Testing Tool for Application Security Testing tool**

The professional should have degree in BE/B.Tech/MCA along with 5 years minimum experience in IT filed with atleast 2 year's experience in Information Security. The professional should have certification in CEH/OSCP along with the hands on experience in working of Application Security Testing tool.

B. **Domain Expert Professional for Penetration Testing Tool**

The professional should have degree in BE/B.Tech/MCA with 5 years minimum experience in IT filed with atleast 2 years' experience in Information Security. The professional should have certification in CEH/OSCP along with the hands on experience in working of Penetration Testing tool.

SCHEDULE OF REQUIREMENT:

Sr. No.	Item	Type	Specifications	Quantity
1	Vulnerability Assessment tool (CVE Complied)	**Testing tool**	Refer clause 2.1	**1**
2	Vulnerability Assessment tool (CCS 7 related)	**Testing tool**	Refer clause 2.1	**1**
3	Fuzzing tool (Ethernet Interface)	**Testing tool**	Refer clause 2.2	**1**
4	Static analysis and dynamic Analysis Application Security Testing tool) **with domain expert professional**	**Testing tool**	Refer clause 2.3	**1**
5	Binary Analysis Tool	**Testing tool**	Refer clause 2.4	**1**
6	Penetration Testing Tool **with domain expert professional**	**Testing tool**	Refer clause 2.5	**1**

Stamp and signature of bidder

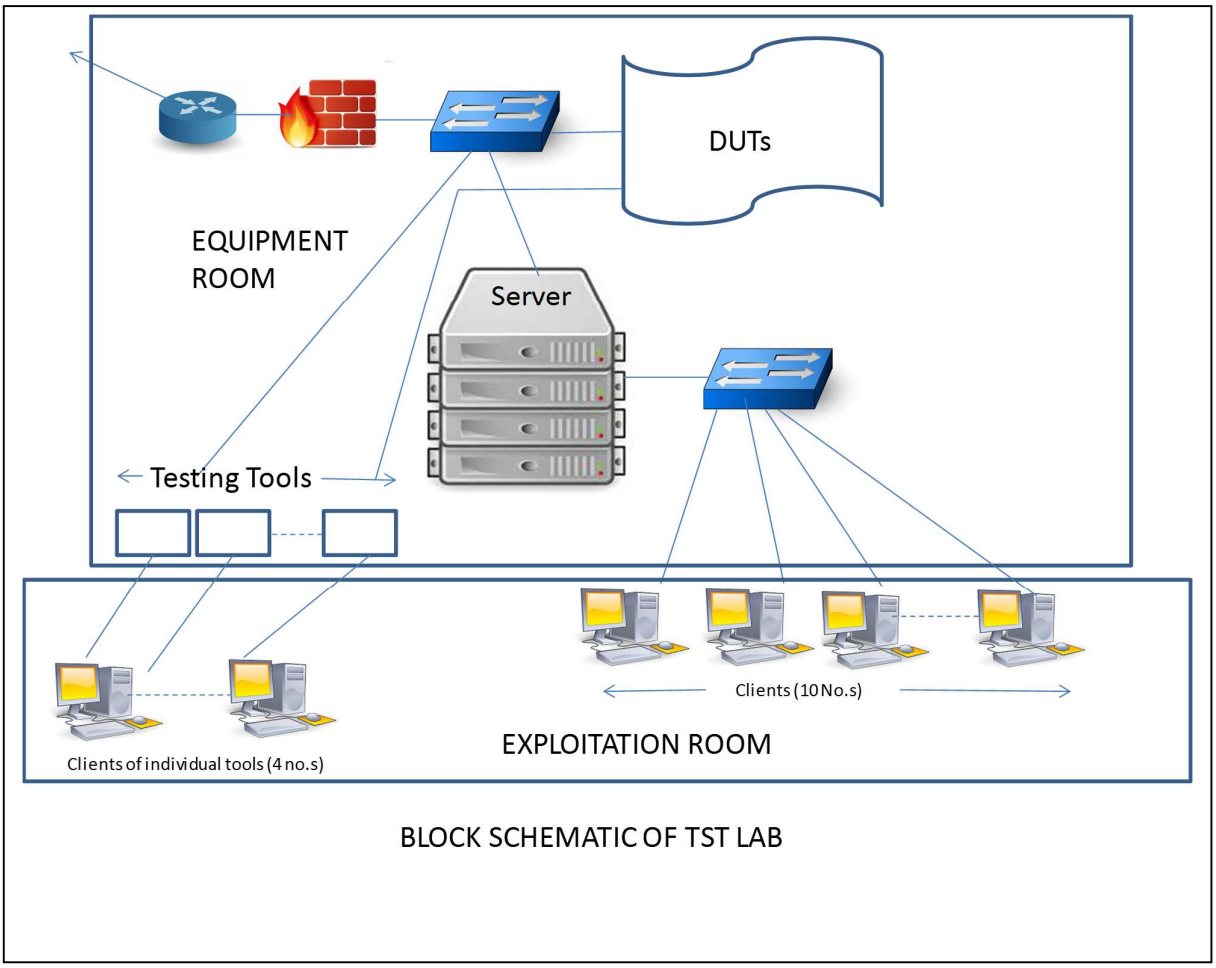

Fig 1: Block Schematic of overall Security Test lab

Stamp and signature of bidder

ANNEXURE - I
PRE-BID/PRE-CONTRACT INTEGRITY PACT

(ON STAMP PAPER OF Rs. 100/-)

This pre-bid pre-contract Agreement (hereinafter called the Integrity Pact) is made on ....., between, on one hand, the President of India acting through ADG (MM) Telecom Engineering Centre, Khurshid Lal Bhawan, Janpath, New Delhi-01 (Designation of the officer, Ministry/ Department, Government of India) (hereinafter called the 'Purchaser'), which expression shall mean and include, unless the context otherwise requires, his successors in office and assigns) of the First Part and
.....
.....
..... represented by
..... on behalf of Chief Executive Officer (Hereinafter called the 'Bidder/Contractor', which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

Whereas the Purchaser proposes to Supply, installation,Testing and Commissioning of Security Testing tools and the Bidder/Contractor is willing to offer has offered the stores and

Whereas the Bidder is a private company/public company/ Government undertaking/ partnership/ registered export agency, constituted in accordance with the relevant law in the matter and the Purchaser is a Ministry/ Department of the Government of India PSU performing its functions on behalf of the President of India.

NOW, THEREFORE,

To avoid all forms of corruption by following a system that is fair, transparent and free from any influence/prejudiced dealings prior to, during and subsequent to the currency of the contract to be entered into with a view to:

Enabling the Purchaser to obtain the desired said stores/equipment at a competitive price in conformity with the defined specification by avoiding the high cost and the distortionary impact of corruption on public procurement, and

Enabling Bidders to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the Purchaser will commit to prevent corruption, in any form, by its officials by following transparent procedures.

In order to achieve these goals, the Purchaser will appoint Independent External Monitors (IEMs) who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

The parties hereto hereby agree to enter into this Integrity Pact and agree as follows:

Stamp and signature of bidder

Section 1- Commitments of the Purchaser

(1) The Purchaser commits itself to take all measures necessary to prevent corruption and to observe the following principles:
a. No employee of the Purchaser, personally or through family members, will in connection with the tender for, or the execution of a contract, demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.

b. The Purchaser will, during the tender process treat all Bidder(s) with equity and reason. The Purchaser will in particular, before and during the tender process, provide to all Bidder(s) the same information and will not provide to any Bidder(s) confidential / additional information through which the Bidder(s) could obtain an advantage in relation to the tender process or the contract execution.

c. The Purchaser will exclude from the process all known prejudiced persons.

(2) If the Purchaser obtains information on the conduct of any of its employees which is a criminal offence under the IPC/PC Act or if there be a substantive suspicion in this regard, the Purchaser will inform the Chief Vigilance Officer and in addition can initiate disciplinary actions.

Section 2 - Commitments of the Bidder(s)/ Contractors(s)

(1) The Bidder(s)/Contractors(s) commit themselves to take all measures necessary to prevent corruption. The Bidder(s)/ Contractors(s) commit themselves to observe the following principles during the participation in the tender process and contract conditions.

(a) The Bidder(s)/Contractors(s) will not directly or through any other person or firm, offer, promise or give to any of the Purchaser's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any advantage of any kind whatsoever during the tender processes during the execution of the contract.

(b) The Bidder(s)/Contractor(s) will not enter with other Bidders into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non-submission of bids or any other actions to restrict competitiveness or to introduce cartelisation in the bidding process.

(c) The Bidder(s)/ Contractors(s) will not commit any offence under the relevant IPC/PC Act; further the Bidder(s)/ Contractors(s) will not use improperly, for purpose of competition or personal gain, or pass on to others. any information or document provided by the Purchaser as part of the business relationship, regarding plans, technical proposals and business details including information contained or transmitted electronically.

Stamp and signature of bidder

(d) The Bidder(s)/Contractor(s) of foreign origin shall disclose the name and address of the Agents/Representatives in India, if any, Similarly the Bidder(s)/Contractors(s) of Indian Nationality shall furnish the name and address of the foreign Purchaser, if any. Further details as mentioned in the "Guidelines on Indian Agents of Foreign Suppliers" shall be disclosed by the Bidder(s)/Contractors(s). Further, as mentioned in the Guidelines all the payments made to the Indian agent/representative have to be in Indian Rupees only.

(e) The Bidder(s)/Contractors(s) will, when presenting their bid, disclose any and all payments made, is committed to or intends to make to spent agents, brokers or any other intermediaries in connection with the aware of the contract.

(f) Bidder(s)/ Contractors(s) who have signed the Integrity Pact shall not approach the Courts while representing the matter to IEMs and shall wait for their decision in the matter.

(2) The Bidder(s)/Contractors(s) will not instigate third person to commit offences outlined above or be an accessory to such offences.

Section 3 Disqualification from tender process and exclusion from future contracts

If the Bidder(s)/Contractor(s), before award or during execution has committed transgression through a violation of Section 2, above or in any other form such as to put their reliability or credibility in question, the Purchaser is entitled to disqualify the Bidder(s)/Contractors(s) from the tender process or take action as per the procedure mentioned in the "Guidelines on Banning of business dealings".

Section 4 - Compensation for Damages

(1) If the Purchaser has disqualified the Bidder(s) from the tender process prior to the award according to Section 3, the Purchaser is entitled to demand and recover the damages equivalent to Earnest Money Deposit/Bid Security.

(2) If the Purchaser has terminated the contract according to Section 3, or if the Purchaser entitled to terminate the contract according to Section 3, the Purchaser shall be entitled to demand and recover from the Contractors liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee.

Section 5 - Previous transgression

(1) The Bidder declares that no previous transgression occurred in the last three years with any other Company in any country conforming to the anti-

corruption approach or with any Public Sector Enterprise in India that could justify his exclusion from the tender process.

(2) If the Bidder makes incorrect statement on this subject, he can he disqualified from the tender process or action can be taken as per the procedure mentioned in "Guidelines on Banning of business dealings".

Section 6 - Equal treatment of all Bidder(s) / Contractors(s) / Subcontractor(s)

(1) In case of Sub-contracting, the Principal Contractors shall take the responsibility of the adoption of Integrity Pact by the Sub-Contractor.

(2) The Purchaser will enter into agreements with identical conditions as this one with all Bidders and Contractors.

(3) The Purchaser will disqualify from the tender process all bidders who do not sign this Pact or violate its provisions.

Section 7 Criminal charges against violating Bidder(s) / Contractors(s) Subcontractor(s)

If the Purchaser obtain knowledge of conduct of Bidder, Contractor or Subject or of an employee or a representative or an associate of a Bidder. Contractor or Subcontractor which constitutes corruption, or if the Purchaser has substantive suspicion in this regard, the Purchaser will inform the same to the Chief Vigilance Officer.

Section 8 - Independent External Monitor

(1) The Purchaser appoints competent and credible Independent External Monitor for this Pact after approval by Central Vigilance Commission. The task of the Monitors is to review independently and objectively, whether and to what extent the party complies with the obligations under this agreement.

(2) The Monitor is not subject to instructions by the representatives of the parties and performs his/her functions neutrally and independently. The Monitor would have access to all Contract documents whenever required. It will be obligatory for him/her to treat the information and documents of the Bidders/Contractors as confidential. He/she reports to the Designated Authority of Purchaser/ Secretary in the department.

(3) The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the Purchaser including that provided by the Contractor. The Contractor will also grant the Monitor, upon his/her request and demonstration of a valid interest, unrestricted and unconditional access to their project documentation. The same is applicable to Subcontractor.

(4) The Monitor is under contractual obligation to treat the info and documents of the Bidder(s)/ Contractors(s) Subcontractors(s) with confidentiality The Monitor has also signed declarations on 'Non-Disclosure of Confidential

Information' and of 'Absence of Conflict of Interest'. In case of any conflict of interest arising at a later date, the IEM shall inform Designated Authority of Purchaser/ Secretary in the department and rescue himself/ herself from that case.

(5) The Purchaser will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meeting could have an impact on the contractual relations between the Purchaser and the Contractor. The parties offer to the Monitor the option to participate in such meetings.

(6) As soon as the Monitor notices, or believe to notice a violation of this agreement, he/she will so inform the Management of the Purchaser and request the Management to discontinue or take corrective action or to take other relevant action. The monitor can in this regard submit non-binding recommendations. Beyond this, the Monitor has no right to demand from the parties that they act in specific manner, refrain from action or tolerate action.

(7) The Monitor will submit a written report to the Designated Authority of Purchaser/ Secretary in the department within 10 weeks from the date of reference or intimation to him by the Purchaser and, should the occasion arise, submit proposals for correcting problematic situations.

(8) If the Monitor has reported to the Designated Authority of Purchaser/ Secretary in the department, a substantiated suspicion of an offence under relevant IPC/ PC Act and the Designated Authority of Purchaser/ Secretary in the department has not within the reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the Monitor may also transmit this information directly to the Central Vigilance Commissioner.

(9) The word 'Monitor' would include both singular or plural.

(10) As per letter no.17-19/2012-VM dated 27 September 2018, the competent authority has appointed the following Independent External Monitors (IEMs) in the Department of Telecommunication for overseeing and implementation of Integrity Pacts in procurements in DoT:

i. Shri Arvind Kumar Arora, Indian Defence Service of Engineers (IDSE),Ex.DG, Indian Defence Engineering Services, Ministry of Defence, B-333, Chittaranjan Park New Delhi-110019 (Tel No. 01126273406, Mob No. 8130588577 & 9868236340,Email ID: arvindarora333@gmail.com)

ii. Shri Pradeep Kumar Gupta, Central Engineering Service. Ex Special Director General, Central Public Works Department, T-17, Green Park Extension, New Delhi-110016 (Tel bo.01126191696, Mobile no. 9971491696, Email-ID: pradeepkgupta53@gmail.com)

Section 9-Pact Duration

This duration of Pact begins when both parties have legally signed the document. It expires for the Contractor 12 months after the last payment under the contract, and for all other Bidders 6 months after the contract has been awarded. Any violation of the same would entail disqualification of the Bidders and exclusion from future business dealings.

If any claim is made/lodged during this time the same shall be binding and continue to be valid despite the lapse of this pact as specified above, unless it is discharged /determined by Designated Authority of Purchaser/ Secretary in the department.

Section 10 - Other provisions

(1) This agreement is subject to Indian Law. Place of performance and jurisdiction is the Registered Office of the Purchaser, i.e. TEC, New Delhi.
(2) Changes and supplements as well as termination notice need to be made in writing. Side agreements have not been made.
(3) The Contractor is a partnership or consortium, this agreement must be signed by all partners or consortium members.
(4) Should one or several provisions of this agreement turn out to be invalid, the remainder of this agreement remains valid. In this case, the parties will strive to come to an agreement to their original intentions.
(5) Issues like Warranty /Guarantee shall be outside the purview of IEMs.
(6) In the event of any contradiction between the Integrity Pact and its Annexure the Clause in the Integrity Pact will prevail.

_____ _____

On behalf of the Purchaser

(For & On behalf of
Bidder/ Contractor)

(Office Seal) (Office Seal)

ANNEXURE - II
INDEMNITY BOND

[To be executed by the Bidder on the Stamp Paper of Rs. 100/-]

1. ……*(Name & address of the bidder)……..* indemnify Telecom Engineering Centre, Department of Telecommunications Khurshid Lal Bhawan, Janpath, New Delhi – 110 001 (hereinafter called TEC) against all third-party claims of infringement of patent, trademark or industrial design rights arising from use of the Security Testing tools, goods or any part thereof, supplied against this tender 2-1/2021-MM/TEC .

2. ……*(Name & address of the bidder)……* indemnify the TEC in respect of any damages, claims, loss or legal action against TEC for acts of commission,(use of Security Tools, hardware and software licenses during and after commissioning) or omission on part of the supplier, its agents or servants.

Signature……
Name……...
Address……..
……

Place:
Date:
Witnesses:

1.

2.

Stamp and signature of bidder

ANNEXURE - III
PROFILE OF BIDDER

1. Full Name of Bidder
2. Registered Address

3. Address of correspondence

4. Details of Contact/Authorized Person
   Name & Designation _____
   Address _____
   Tel No. (Landline) _____ Mobile _____
   Email ID _____FAX:_____
5. Type of Firm: Private Ltd./Public Ltd./Co-operative/PSU/Proprietary
   (Please tick the appropriate)
6. Name(s) of Directors/ partners/ proprietor

7. PAN/GIR No. : _____

8. TIN No. : _____

9. GST Registration No.: _____

10. Proof of Annual Turnover of As specified in table or more:

11. Earnest money details: DD No. _____ dated _____ for Rs…….. drawn on _____
12. Bank Account details of the bidder:
    a. Name and address of Bank
    b. Account no.
    c. MICR no.
    d. IFSC code of Branch
13. Any other relevant information:

(Signatures of authorized signatory)
Name_____
Designation_____
Seal:

Stamp and signature of bidder

ANNEXURE - IV
EMD BG FORM

Whereas _____ (hereinafter called the *Bidder*) has submitted its bid dated _____ for the Supply, installation,Testing and Commissioning of Security Testing tools against Tender Enquiry No. 2-1/2021-MM/TEC dated 06.10.2021, know all men by these presents that we _____ of _____ having our registered office at _____ _____ (hereinafter called the *Bank*) are bound unto the Sr. DDG, TEC (hereinafter called the *Purchaser*), for the sum of…….. (As specified in NIT)/- for which payment will and truly be made to the Purchaser, the Bank binds itself, its successors, and assigns by these presents.

The conditions of the obligation are

1. If the Bidder withdraws its bid during the period of the bid validity as specified by the Bidder on the Bid Form, or
2. If the Bidder, having been notified of the acceptance of its bid by the Purchaser, during the period of bid validity
   a. Fails or refuses to execute the contract, if required, or
   b. Fails or refuses to furnish performance security, in accordance with the Instructions to the Bidders.

We undertake to pay the Purchaser up to the above amount upon receipt of its first written demand without the Purchaser having to substantiate its demand, provided that in its demand, the Purchaser will note that the amount claimed by it is due to it owing to the occurrence of one or both of the two conditions, specifying the occurred condition(s).

This guarantee will remain in force as specified in the Instruction to the Bidders, for the period 285 days from the date of opening of bid or any other date as extended, and any demand in respect thereof should reach the Bank not later than the specified date(s).

Dated the ---------- day of ----------, Two thousand one only.

For ----------
(Indicate the name of the bank)

Witnesses:-

1. Telephone No.(s):-
   STD Code-
   FAX No.
   E-Mail Address:-

2.

Stamp and signature of bidder

ANNEXURE - V
NO NEAR-RELATIVE DECLARATION/CERTIFICATE

(To be submitted by either authorized signatory or proprietor, or each partner/director in case of partnership firms/companies)

I _____ son/daughter/wife of

Shri _____

_____Proprietor/Partner/Director/Authorised signatory/Representative of M/s _____

(Name and address of the bidder) is competent to sign this declaration and execute the tender document regarding "Supply, installation,Testing and Commissioning of Security Testing tools at TEC New Delhi";

I _____ resident of _____ hereby certify that none of relatives of mine/proprietor/partners/directors is/are employed in the units where he/she is going to apply for the tender. In case at any stage it is found that the information given by me is false/incorrect the purchaser shall have the absolute right to take any action as deemed fit/without any prior information to me.

I have carefully read and understood all the terms and conditions of the tender document and undertake to abide by the same;

I also undertake that our firm will observe all legal formalities or/and obligations under the contract well within time. In case of failure to observe any of the legal formalities or/and obligations. I shall be personally liable under the appropriate law.

The Information/documents furnished, along with the tender document are true and authentic to the best of my knowledge and belief. I am well aware of the fact that furnishing of any false information/fabricated documents would lead to rejection of my tender at any stage besides liabilities towards prosecution under appropriate law.

(Signature of Proprietor/Partners/Director/Authorized Signatory)

Full Name:

Date: Address:

Place: Seal:

ANNEXURE - VI
PERFORMANCE SECURITY BOND FORM

In consideration of the President of India (hereinafter called 'the Government') having agreed to exempt ---------- (hereinafter called 'the said Contractor(s)' from the demand, under the terms and conditions of an agreement / (Purchase Order) No. ---------- Dated ---------- made between ---------- and ---------- for the supply and Service Level Agreement (SLA) of ---------- (hereinafter called 'the said Agreement'), of performance security for the due fulfilment by the said Contractor(s) of the terms and conditions contained in the said Agreement, on Production of a bank guarantee for ---------- we, (Name of the bank) ---------- (hereinafter referred to as 'the Bank') at the request of ---------- contractor(s) do hereby undertake to pay to the TEC an amount not exceeding ---------- against any loss or damage caused to or suffered or would be caused to or suffered by the TEC by reason of any breach by the said Contractor(S) of any of the terms or conditions contained in the said Agreement.

2. We (Name of the bank) ---------- do hereby undertake to pay the amount due and payable under this guarantee without any demur, merely on a demand from the TEC stating that the amount claimed is due by way of loss or damage caused to or would be caused to or suffered by the TEC by reason of the contractor(s) failure to perform the said Agreement. Any such demand made on the bank shall be conclusive as regards the amount due and payable by the Bank under this guarantee where the decision of the TEC in these counts shall be final and binding on the bank. However, our Liability under this guarantee shall be restricted to an amount not exceeding ----------.

The Bank further agrees that the guarantee herein contained shall remain in full force and effect for a period of 7 years & 6 Months from the date hereof and also that the extension of this guarantee will be provided for by the Bank for such period beyond the period of 7 years & 6 Months as the Purchaser may feel necessary in this behalf.

3. We undertake to pay to the TEC any money so demanded notwithstanding any dispute or disputes raised by the contractor(s)/ supplier(s) in any suit or proceeding pending before any court or tribunal relating thereto our liability under this present being absolute and unequivocal. The payment so made by us under this bond shall be valid discharge of our liability for payment there under and the contractor(s)/ supplier(s) shall have no claim against us for making such payment.

4. We (name of the bank) ---------- Further agree that the guarantee herein contained shall remain in full force and effect during for a period of 7 years & 6 Months from the date of Advance Purchase Order (Date……..). And that it shall continue to be enforceable till all the dues of the TEC under or by virtue of the said Agreement have been fully paid and its claims satisfied or discharged or till ---------- (TEC) certifies that the terms and conditions of the said Agreement have been fully and properly carried out by the said contractor(S) and accordingly discharge this guarantee.

5. We (Name of the bank) ---------- further agree with the TEC that the TEC shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary and of the terms and conditions of the said Agreement

Stamp and signature of bidder

or to extend time of performance by the said contract(s) from time to time or to postpone for any time or from time to time any of the powers exercisable by the TEC Against and said Contract(s) and to forbear or enforce any of the terms and conditions relating to the said agreement and we shall not be relieved from our liability by reason of any such variation, or extension being granted to the said Contract(s) or for any forbearance, act or omission on the part of the TEC or any indulgence by the TEC to the said contract(s) or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have effect of so relieving us.

6. This guarantee will not be discharged due to the change in the constitution of the Bank or the contractor(s)/ supplier(s).

7. We (name of the bank) ---------- lastly undertake not to revoke this guarantee during its currency except with the previous consent of the TEC in writing.

Dated the ---------- day of ----------, Two thousand one only.

For ----------
(Indicate the name of the bank)

Witnesses: (Name & Signature)

1. Telephone No.(s):-
STD Code-
FAX No.
E-Mail Address:-

2.

Stamp and signature of bidder

ANNEXURE - VII
BID FORM

2-1/2021-MM/TEC
Dated: 06.10.2021

To
The Sr. DDG,
TEC, New Delhi.

Dear Sir,

Having examined the conditions of tender and specifications including clarifications/addenda the receipt of which is hereby duly acknowledged, we, the undersigned, offer to supply and deliver the item(s) quoted in Price Schedule of this bid document in conformity with said conditions of contract and specifications for a sum of amount as quoted in Price Schedule or such other sums as may be ascertained in accordance with the schedule of prices and made part of this Bid.

We undertake, if our Bid is accepted, to commence and complete deliveries as prescribed in the tender document.

If our Bid is accepted, we will obtain and provide to purchaser the guarantees of a Scheduled Bank for a sum not exceeding 10% of the contract sum for the due performance of the Contract.

We agree to abide by this Bid for a period of 240 days from the date fixed for Bid opening and it shall remain binding upon us and may be accepted at any time before the expiration of that period.

Bid submitted by us is properly sealed and prepared so as to prevent any subsequent alteration and replacement.

We understand that you are not bound to accept the lowest or any bid, you may receive.

Dated this .....day of 2019

(……)

Signature of…….

in capacity of…….
(Duly authorized to sign the bid for and on behalf of.....)

Witness.....

Signature.....

Address.....

Tele No.(s):-

FAX No.(s):-

E-Mail Address:-

Stamp and signature of bidder

ANNEXURE –VIII
TECHNICAL BID Summary Form

a) Security Tools with associated hardware offered

Sl. No.	Item Description	Quoted for Tool(YES/NO)	Tool Name & OEM	Software Version of the Tool Offered	Associated Hardware details for tools offered	OEM Authorisation for tool Submitted (YES/NO)	Page Reference to related documents in Technical Bid
1.	**Vulnerability Assessment tool** (CVE complied)						
2.	**Vulnerability Assessment tool** (CCS7 related)						
3.	**Fuzzing tool** (Ethernet Interface)						
4.	**Security Testing tool for application(Static analysis and dynamic Analysis Security Testing tool)**						
5.	**Binary Analysis Tool**						
6.	**Penetration Testing Tool**						

b) Key document check list

(This check list is only an indicative list. Bidders are required to read the tender document carefully and submit all the documents/details required for Technical evaluation as per clause 7.0, Section II of tender document)

Sl. No	Tender Clause Reference	Documents Submitted (Yes/No)	Page Reference in Technical Bid
1.	Clause 2.2,Section II		
2.	Clause 2.3,Section II		
3.	Clause 2.4,Section II		
4.	Clause 2.5,Section II		

Stamp and signature of bidder

5.	Clause 9.4,Section II		
6.	Clause 17.1,Section II		
7.	Signed tender document along with all annexure and amendments/clarifications		
8.	PAN Card/GIR Card and GST Registration certificate		
9.	All Annexures [I to XII]		
10.	List of software including licences etc., necessary for the proper and continuous functioning of the offered solution tool(s) along with undertaking that all the software including licenses as indicated above are being proposed to be supplied in the bid are of perpetual nature.		
11.	List of Partners/directors of the bidder along with Partnership Deed or Article/Memorandum of Association		
12.	OEM certificate stating that all software supplied are authentic and legal copy is/are being supplied		

Stamp and signature of bidder

ANNEXURE - IX
LIST OF PROTOCOLS AND FILE FORMATS

LIST A of FUZZER-E:

Sl No.	Protocol Name	Protocol Description
1.	ARP	Address resolution protocol
2.	BGP4	Border Gateway protocol
3.	DIAMETER	Authentication, Authorization and Accounting Protocol (Evolved form of RADIUS)
4.	DHCP	Dynamic Host Configuration Protocol
5.	DHCPv6	Dynamic Host Configuration Protocol version 6
6.	FTP	File Transfer Protocol
7.	H.248	Megaco
8.	HTTP 1.0,HTTP 1.1	Hyper Text transfer protocol
9.	HTTPS 1.0, HTTPS1.1	HTTP Over TLS/SSL
10.	ICMP	Internet Control Message protocol
11.	ICMPv6	Internet Control Message protocol v6
12.	IGMP v2 and v3	Internet Group Management Protocol
13.	IMAP	Internet message access protocol
14.	IPsec - IKEv2	Internet key exchange ver.2 of IPsec protocol suit
15.	IPv4	Internet Protocol v4
16.	IPv6	Internet Protocol v6
17.	LDAPv3	Lightweight directory access protocol ver.3
18.	LLDP (802.1ab)	Link-layer discovery protocol
19.	MGCP	Media Gateway Control protocol
20.	NTP	Network Time Protocol, Simple Network Time Protocol
21.	OSPFv2 ,OSPFv3	Open Shortest path first ver.2 and ver.3
22.	PIM-SM	Protocol Independent Multicast sparse mode
23.	POP 3	Post office protocol
24.	PPPoE	Point to point over Ethernet

Stamp and signature of bidder

25.	RADIUS	Remote Authentication Dial-In User Service
26.	RIP v2 , RIPng	Routing Information protocol
27.	RTCP	Real Time control Protocol
28.	RTP	Real Time Protocol
29.	RTSP	Real time streaming protocol
30.	SCTP	Stream control transmission protocol
31.	SIP(IETF Profile)	Session Initiation Protocol
32.	SMTP	Simple mail transfer protocol
33.	SNMP v1,SNMP v2, SNMP v3	Simple Network Management Protocol
34.	SSH	Secure Shell
35.	SSL	Secure Socket Layer
36.	TCP	Transmission Control Protocol
37.	Telnet	
38.	TFTP	Trivial File Transfer Protocol
39.	TLS	Transport Layer Security
40.	UDP	User datagram Protocol
41.	Wifi (IEEE 802.11 n)	
42.	SMB	Server Message Block
43.	DNS	Domain Name System

File Formats	
1.	GIF(Image format)
2.	JPEG(Image format)
3.	PNG (Image Format)
4.	TIFF (Image Format)
5.	WAV (Audio Format)

Stamp and signature of bidder

LIST B of FUZZER-E:

Sl No.	Protocol Name	Protocol Description
1.	BICC	Bearer Independent call control
2.	BICC-CS2	Bearer Independent Call control Capability set 2
3.	Bluetooth Family (version 4.0,4.1,4.2)	
4.	BOOTP Vendor Extensions as per RFC 2132	BootStrap Protocol
5.	CAP	Customized Applications for Mobile Network Enhanced Logic Application protocol
6.	CHAP and CHAP v2	Challenge handshake Authentication Protocol
7.	DHCP Options v4 v6	Dynamic Host configuration Protocol Options
8.	DTAP	Direct Transfer Application Part
9.	DVMRPv1, DVMRPv3	Distance Vector Multicast Routing Protocol
10.	FCOE	Fibre Channel over Ethernet protocol (INCITS FC-BB-5)
11.	GTP-U	GPRS Tunneling protocol – user plane
12.	GTP-C	GPRS Tunneling protocol – control plane
13.	H.323	ITU-T recommendation that defines the protocols to provide audio visual communication sessions on packet networks
14.	IEEE 802.3	
15.	IEEE 802.3ad	
16.	INAP	Intelligent Network Application Part

Stamp and signature of bidder

17.	IPsec – AH	Authentication header of IPsec protocol suit
18.	IPsec – ESP	Encapsulating Security Payloads of IPsec protocol suit
19.	Iscsi	Internet Small Computer System Interface
20.	ISUP (including SS)	ISDN User part (including Supplementary Services)
21.	L2CP	Layer 2 Control Protocol
22.	L2TP	Layer 2 Tunneling protocol
23.	LCP	Link control protocol
24.	LDP	Label distribution protocol (Used in MPLS Routers)
25.	LLC	Logical link control (IEEE 802.2)
26.	M2PA	Message Transfer Part 2 (MTP) Peer-to-Peer Adaptation Layer
27.	M2UA	MTP2 User Adaptation Layer
28.	M3UA	MTP level 3 User Adaptation
29.	MAC	Media Access Control
30.	MAP	Mobile Application Part (SS7)
31.	MBGP	Multiprotocol or Multicast Border Gateway Protocol
32.	MLDv1 , MLDv2	IPv6 Multicast Listener Discovery protocol
33.	MSRP	Message session relay protocol
34.	MSDP	Multicast Source Discovery Protocol
35.	MTP	Message Transfer part of SS7
36.	NAS	Non Access Stratum
37.	NFS	Network File system
38.	OSI ISIS	Intra-domain Routing Protocol
39.	PAP	Password Authentication Protocol

40.	PIM SSM	PIM Source Specific Multicast
41.	PTPv2	Precision Timing Protocol
42.	RANAP	Radio Access Network Application Part
43.	RMON	Remote Network Monitoring
44.	RSVP	Resource reservation protocol
45.	S1-AP	S1-Application Protocol (Signalling interface between EUTRAN and EPC of LTE)
46.	SCCP	Signaling connection control part
47.	SFTP	Secure File Transfer Protocol
48.	SDP	Session Description Protocol
49.	SIP (3GPP Profile)	Session Initiation Protocol
50.	SIP-I	Session Initiation Protocol with Encapsulated ISUP
51.	SMS (User /Network)	
52.	SOAP	Simple Object Access Protocol
53.	Spanning Tree Protocol	IEEE 802.1D
54.	STUN	Simple Traversal of user datagram protocol
55.	SUA	SCCP User Adaptation Layer
56.	SDN related protocols (Software defined networking related protocols)	Open flow Protocol
57.	TACACS+	Terminal Access Controller Access Control System
58.	TCAP	Transaction Capabilities Application Part (SS7)
59.	VRRP	Virtual Router Redundancy Protocol
60.	XCAP	XML configuration Access protocol

Stamp and signature of bidder

61.	XML	Extensible Markup Language
62.	X2-AP	X2- Application protocol (UE mobility between EUTRAN of LTE)
63.	BSSAP	BSS Application Part
64.	BSSAP+	BSS Application Part plus
65.	BSSGP	BSS GPRS Protocol
66.	BSSMAP	BSS management Application part

File Formats	
1.	AMR (Audio format)
2.	ANI (Image format)
3.	AIFF (Audio format)
4.	AU (Audio format)
5.	AVI(Video format)
6.	BMP (Image format)
7.	CAB (Archive format)
8.	DOC (MS Word file)
9.	GZIP(Archive format)
10.	HTML
11.	ICO (Image format)
12.	IMY(Audio format)
13.	JAR (Archive format)
14.	JASC PAL
15.	LHA(Archive format)
16.	MBM(Image format)
17.	MOV(Video format)
18.	MP3(Audio format)
19.	MPEG1 (Video format)
20.	MPEG2(Video format)
21.	MPEG2-TS (Video format)
22.	MPEG4 (Video format)
23.	PAL
24.	PCX(Image format)
25.	PDF
26.	PIX(Image format)
27.	PNM(Image format)
28.	PPT (MS Power Point)
29.	Quick Time (Multimedia Container File)
30.	RAS(Image format)

31.	TGA(Image format)
32.	UPnP (Universal Plug n Play)
33.	UPX(Image format)
34.	VOC(Audio format)
35.	WBMP(Image format)
36.	WMF(Image format)
37.	XBM(Image format)
38.	XLS (MS-Excel)
39.	XPM(Image format)
40.	ZIP (Archive format)

ANNEXURE - X
NO BLACKLISTING DECLARATION/CERTIFICATE

(To be submitted by either authorized signatory or proprietor, or each partner/ director in case of partnership firms/companies)

I _____ son/ daughter/ wife of Shri _____Proprietor/ Partner/ Director/ Authorised signatory/ Representative of M/s _____
(Name and address of the bidder) is competent to sign this declaration and execute the tender document regarding "Supply, installation,Testing and Commissioning of Security Testing tools at ";

I _____ resident of _____ hereby certify that our company has not been black-listed by any Ministry/ Department/ PSU of the Central Government. In case at any stage it is found that the information given by me is false/ incorrect the purchaser shall have the absolute right to take any action as deemed fit/without any prior information to me.

I have carefully read and understood all the terms and conditions of the tender document and undertake to abide by the same;

I also undertake that our firm will observe all legal formalities or/and obligations under the contract well within time. In case of failure to observe any of the legal formalities or/and obligations, I shall be personally liable under the appropriate law.

The Information/documents furnished, along with the tender document are true and authentic to the best of my knowledge and belief. I am well aware of the fact that furnishing of any false information/fabricated documents would lead to rejection of my tender at any stage besides liabilities towards prosecution under appropriate law.

(Signature of Proprietor/ Partners/ Director/ Authorized Signatory)

Full Name:

Date: Address:

Place: Seal:

Stamp and signature of bidder

ANNEXURE - XI
OEM Authorization Form

To,
The Sr. DDG,
TEC, New Delhi.

WHEREAS [name of the OEM] who are established and reputable manufacturers of [name and/or description of the Security tool/goods] having factories at [address of factory/Software Development Centre]

do hereby authorize [**name and address of Bidder**] is an authorized supplier of the ……(respective OEM(s)) and ……(respective OEM's) commits for successful supply, installation, acceptance testing, warranty, updation, upgradation, accreditation support and SLA of testing tool(s) for the entire period of contract against Tender no.2-1/2021-MM/TEC dated 06.10.2021 for the above mentioned Security tool/goods manufactured by us.

_____
[Signature for and on behalf of OEM]

Note: This letter of authority should be on the letterhead of the OEM and should be signed by a person competent and having the power of attorney to bind the OEM. It should be included by the Bidder in its Technical bid.

Stamp and signature of bidder

ANNEXURE - XII
Technical Compliance Sheets

1. Vulnerability Assessment Tool:

S no.	Clause	Complied (Yes/No)
I.	There shall be 2 types of Vulnerability assessment tools, One CVE compliant and other for CCS-7 related testing.	
II.	Vulnerability assessment tool supplied shall be capable of scanning targets i.e. network nodes including end user devices, the operating systems, databases, and/or Web applications residing on those nodes in an attempt to detect known vulnerabilities.	
III.	The identified vulnerabilities shall comply to latest CVE catalogue as well as any other telecom vulnerabilities in access network and core network and end user devices including any other prevalent standard at the time of placement of purchase order as per standard catalogue available publicly and commercially.	
IV.	The supplied Vulnerability assessment tool shall be capable of doing the scanning of individual devices connected to the tool on one to one basis and / or a range of devices connected to the tool through LAN as well as WAN network.	
V.	The supplied tool shall begin its assessment by performing a "footprint" analysis that involves first discovering all open ports on a device under test, then scanning these ports to enumerate all of the available services on the device to determine which services and/or software programs (including versions and patch levels) are running on the target. The tool shall also have the capability of assessing by "footprint" analysis of first discovering all active nodes on the network, then scanning them to enumerate all of the available network services on each host to determine which network services and/or software programs (including versions and patch levels) are running on the target. Then the supplied tool shall attempt to identify (patterns/ attributes of) the known vulnerabilities, in the detected services/software versions, and then report their findings as result.	

Stamp and signature of bidder

VI.	Active scanning i.e. scanning followed by validation of the detected vulnerabilities shall be performed by the supplied tool to verify that those vulnerabilities are, in fact, both present as well as exploitable. The tool shall be capable of analyzing false positives i.e., the instances in which the scanner detects a pattern or attribute indicative of a likely vulnerability, which upon further analysis proves to be either not present or not exploitable.	
VII.	The supplied Vulnerability Assessment tools shall be capable of scanning a number of network nodes, both local and remote, including networking and networked devices (Mobiles, Modems, set top box etc. switches, routers, firewalls, printers, etc.), as well as server, desktop, and portable computers.	
VIII.	The tool shall be able to schedule scans at specific starting dates and time, frequencies and maximum scan durations.	
IX.	The tool shall be able to automatically pause scheduled scans if unable to complete within the predefined durations.	
X.	Each purchased single user license of the tool shall support testing of at least 20 devices simultaneously.	
XI.	The tool shall be upgrade the IP license to a larger in case need to scan more IPs.	
XII.	The tool shall be able to support both credentialed and non-credentialed scans which include but is not limited to: SNMP, SSH, WINDOWS.	
XIII.	The tool shall run on Windows, Linux (all distributions) OS operating environment.	
XIV.	The tool must support the automatic discovery of virtual assets on VMware.	
XV.	The tool must support integration with IDS/IPS products.	

Stamp and signature of bidder

XVI.	The reports generated by the supplied vulnerability assessment tool shall also provide categorization/prioritization, exact remediation for individual vulnerabilities, and recommendations on how to fix and improve the security of the DUT / EUT and overall network in line with the best practices.	
XVII.	The tool shall be able to integrate native exploit information from wellknown sources, minimally with ExploitDB and Metasploit database.	
XVIII.	The tool shall support integration with external penetration testing platforms to perform and automatic vulnerabilities exploitation.	
XIX.	The tool shall be able to identify known exploits and malware kits associated with detected vulnerabilities.	
XX.	There shall not be any need to load or maintain any client software on the targets i.e. device under test.	
XXI.	The vulnerability knowledge database for this tool shall comprise of all the published vulnerabilities as per latest CVE catalogue including any other prevalent standard at the time of placement of purchase order as per standard catalogue available publicly and commercially. The supplier shall ensure the upgradation of library of known vulnerabilities on a weekly basis in complete synchronization with the vulnerabilities published in the CVE catalogue as well as any other the telecom vulnerabilities catalogue.	
XXII.	The library of the vulnerability assessment tools shall be updated on a regular basis with the most recent security vulnerabilities and shall contain a complete trigger list of all possible known attacks e.g. DDoS, Buffer overflow, SQL injection, eavesdropping, session hijacking, APT, BOTs etc.	
XXIII.	The tool shall be coded with maximum coverage of plugin's (which is a simple program that checks for a given flaw) covering of local and remote flaws.	

Stamp and signature of bidder

XXIV.	The tool shall be able to perform both automatic & manual (Plugins/ Software updates).	
XXV.	The tool shall identify misconfigurations in target device like missing patches in OS/applications etc.	
XXVI.	The tool shall support integration with Active Directory, Kerberos, or any LDAP compliant directory.	
XXVII.	The tool shall be with web application scanning solution must support coverage of latest OWASP vulnerabilities.	
XXVIII.	It shall be capable of scanning all the operating systems, firmware, databases, protocols and applications being used by telecom equipment including smartphones, tablets, dongles, modems, all types of wireless access points, routers, switches and perimeter devices e.g. firewalls, IDSs, IPSs, UTMs etc.	
XXIX.	The supplier shall provide suitable on-site mechanism to customize the format of the report generated by the tool as per the requirement of the purchaser.	
XXX.	The tool shall be upgraded by the supplier with capabilities for scanning new operating systems, firmware, databases, protocols and applications being used by telecom equipment including smartphones, tablets, dongles, modems, all types of wireless access points within 3 months from the date of request by the purchaser.	
XXXI.	The tool shall provide user friendly interface for testing and report generation.	
XXXII.	It shall be possible to access the tool and conduct testing lifecycle from the User interface from the desktop client	
XXXIII.	It shall be possible to store and transfer the test results to the test result repository server in the network for record keeping.	

Stamp and signature of bidder

2. Fuzzing tool:

S no.	Clause	Complied (Yes/No)
I.	Fuzzer-E shall comply with generation based fuzzing of protocols mentioned in list A and list B of Annexure and. In case CCS7 protocols of List A and List B are not possible to be tested through Ethernet based Fuzzer, then separate tool shall be provided for CCS7 protocols at no extra cost to the purchaser along with Ethernet based Fuzzer.	
II.	Fuzzing tool shall be capable of discovering unknown / zero day vulnerabilities in a target by providing unexpected inputs towards it and monitoring the target for exceptional behavior.	
III.	It shall be capable of doing *generation-based fuzzing* as well as *mutation-based fuzzing.* Generation-based fuzzing tools create test cases from scratch by modeling the target protocol or file format. Mutation-based fuzzing tool here means that the fuzzing tool, which apply mutations on captured data samples to create test cases.	
IV.	Fuzzer-E shall be capable of doing the following types of fuzzing in a fully automated manner: *a.* Protocol fuzzing for protocols mentioned in Annexure IX being used in telecom network nodes as well as end user devices. *b.* Operating system and firmware fuzzing. *c.* Application fuzzing for all applications running in client devices (e.g. smart phones) as well as those hosted on servers. *d.* Web browser fuzzing to uncover the bugs in web browsers. *e.* File format fuzzing to detect the unknown vulnerabilities present in maliciously crafted files for the file formats mentioned in list A and list B of Annexure.	

Stamp and signature of bidder

V.	Protocol fuzzing done by the supplied tool shall be dynamic and stateful with in-built complete protocol state machines that enable robustness testing deep within the target protocol's software layers and state transitions. It shall support fuzzing throughout every message exchange and transition that a protocol supports in a real operating environment.	
VI.	All the standard protocols including custom and proprietary extensions shall be supported. Addition of new protocols to this tool in future shall also be supported within six months from the date of request by the purchaser.	
VII.	Other than detecting the hard crashes, the supplied fuzzing tool shall be capable of detecting and reporting the soft faults e.g. delayed response. Any other capability of detecting and reporting faults shall be listed by the supplier along with the bid.	
VIII.	The supplied fuzzing tool shall also monitor the behaviour of the device under test (DUT), and correlate cause and effect between the specific negative test case(s) and the abnormal behaviour. For every such fault identified, it shall perform automated data collection, alerting and reporting. It shall enable the user to implement the reproduction of bugs identified. The tool shall support both in-band and out-of-band instrumentation. In-band instrumentation is used to obtain the crash - no crash status and usually consists of sending a valid protocol request to the DUT. The tool shall support both SNMP checks and Syslog checks as out-of-band instrumentation methods used to obtain DUT state information.	
IX.	Tool shall be capable of identifying the following responses of the DUT to the fuzz testing: • The DUT crashes and is unable to restart • The DUT crashes and then possibly restarts.	

Stamp and signature of bidder

	• The DUT hangs in a busy loop, causing a permanent Denial of Service situation. • The DUT slows down momentarily causing a temporary Denial-of- Service situation. • The DUT fails to provide useful services causing a Denial-of-Service situation (i.e. new network connections are refused)	
X.	It shall be possible for the tester to choose the test cases to be run as per need, based on protocol PDU fields, message type, etc. It shall also be possible for the tester to run the most effective attack patterns for different fields of the protocol to keep the test run time reasonable.	
XI.	The tool should be capable of checking interoperability between Test tool and DUT for all the protocols mentioned in Annexure A and Annexure B.	
XII.	The tool should be installable and executable on all popular operating Systems platforms with 32 bit and 64 bit versions (on personal Computers).	
XIII.	It shall have a user-friendly graphical user interface as well as command line interface for handling and operation of the Fuzzing techniques supported and the analytical abilities provided. A very well documented user manual shall be made available for this purpose.	
XIV.	The supplier shall ensure that in case of power failure or abrupt shutdown, the fuzzer tool shall resume the testing from the point at which the shutdown occurred. It should not happen that the tool starts performing the fuzzing from the beginning unless required by the user / purchaser.	
XV.	The generated reports shall also provide prioritization of the detected vulnerabilities highlighting the most critical problems first. It shall be able to capture critical details from the DUT during the fault event or crash, and	

Stamp and signature of bidder

	provide actionable remedies along with packet captures (PCAPs) and External Vulnerability Triggers / exploits.	
XVI.	The tools shall maintain a detailed log of the fuzz testing and it shall be possible for the tester to access the log details at any time. It shall be possible to export the log file to an external storage in standard file formats that will enable viewing of the test information at any point of time.	
XVII.	A single license of Fuzzer shall provide simultaneous testing of atleast 20 devices, of all the protocols, file formats, operating system, firmware, web browser.	
XVIII.	All the file formats and protocols mentioned in Protocol List A for the Fuzzer E of the Annexure, shall be essentially supported at the time of submission of bid. However, the Supplier shall be required to comply with List B (as applicable) of Annexure within 365 days from date of placement of PO. In case a DUT offered in SECURITY TEST Lab requires testing of any file formats and protocols mentioned in List B for Fuzzer-E, purchaser reserves the right to demand support for one or more protocols mentioned therein. The supplier shall have to comply this within three months from the date of request by the purchaser.	
XIX.	The supplier shall provide a suitable on-site mechanism to customize the format of the report generated by the tool as per the requirement of the purchaser.	
XX.	The supplied tool shall be upgraded by the supplier for the latest telecom protocols in access, transport, control and application layers of wireless and wire line domain including 4G and 5G	

Stamp and signature of bidder

	protocols during the entire contract period.	
XXI.	For the remaining protocols, the supplied tool shall be upgradable and supplier shall provide the required tools/SDK for development of generation based fuzzing for telecom protocols defined in ITU-T,3GPP, IETF etc. and generation/mutation based fuzzing for all the custom and proprietary extensions and mutation based fuzzing for any identified protocols as per request made by purchaser.	
XXII.	It shall be possible to access the tool and conduct testing lifecycle from the User interface from the desktop client.	
XXIII.	It shall be possible to store and transfer the test results to the test result repository server in the network for record keeping.	

3. Static Code Analysis Tool and Dynamic Application Security Testing Tool (DAST):

3.1 Static Code Analysis Tool:

S no.	Clause	Complied(Yes/No)
I.	The supplied tool shall be capable of automatically scanning source code of any type to identify the exact locations of security vulnerabilities that can be exploited. It shall scan the source code vulnerabilities against all the prevalent security coding vulnerability databases (e.g. CWE, SANS TOP 25, OWASP TOP 10, CVE).	
II.	It shall correlate and prioritize results to deliver an accurate, risk-ranked list of issue along with corresponding CWE code to ensure that the most serious issues are	

Stamp and signature of bidder

	addressed first. It shall provide detailed guidance on how to fix the vulnerabilities at the line-of-code level.	
III.	It shall be a platform independent tool and support variety of operating systems such as Windows, Linux, MacOS and should allow scanning of different coding languages used in software/firmware of telecom/ICT products, CPEs, mobile phones, applications etc. without installing and updating the respective compilers.	
IV.	The supplied tool shall be capable of checking the source code compliance as per the secure coding standards e.g. Cert C, Cert Java, Cert C++, CWE Database, ISO/IEC TS 17961 and any other coding standards prevalent on the date of placement of purchase order of this tool covering the devices mentioned in clause 2.3.1(iii). In addition to this, it shall be possible to customize the tool for a user defined coding standard i.e. the standards adapted by the manufacturers of the DUTs.	
V.	It shall be capable of detecting malicious code insertion, which may result into exploitation of array bound overflow and buffer overflow	
VI.	It shall have a user-friendly graphical user interface for all programming languages. A web based GUI along with CLI is preferred	
VII.	The tool shall generate reports like: a. Summary reports (e.g.: Vulnerability category wise reports (memory leaks, API abuse, buffer overflow and so on), Severity wise reports, Configuration reports) b. Technical Detailed Report providing all the details of the identified vulnerabilities like category of the Vulnerability, CWE code, Location of the Vulnerability including file name and line number of code, Remediation advice along with code samples in the same programming language and so on.	
VIII.	The tool shall capable of generating the report in standard format and supplier shall provide a suitable on-site mechanism to	

	customize the format of the report generated by the tool as per the requirement of the purchaser.	
IX.	The supplied tool shall be updated and upgraded with new versions of all the coding languages supported by the tool during the entire period of contract.	
X.	The supplied tool shall also be upgraded with new coding languages/ scripts/ structures etc. used in the telecom or IT software/ firmware domain within 3 months from the date of request by the purchaser.	
XI.	It shall provide compliance against any new/ modified international coding standards within 3 months from the date of request by the purchaser.	
XII.	It shall be updated to provide compliance for all the new additions in OWASP, SANS and CWE standards of coding weaknesses within a 15 days' time frame from the date of release of such additions.	
XIII.	It shall be capable to identify Control flow, Pattern/rule based analysis and Data flow anomalies like Un-initialized variables, defined but unused variables, defined then defined again without being used, etc.	
XIV.	It shall be capable to do Information Flow analysis to identify inter dependencies of programming variables like strong/ weak dependencies, Direct/ Indirect dependencies and Conditional/Unconditional dependencies.	
XV.	It shall be capable to do structural coverage analysis to measure what code has been executed	

Stamp and signature of bidder

XVI.	The tool shall have an acceptably low false positive rate.	
XVII	It shall be possible to access the tool and conduct testing lifecycle from the User interface from the desktop client.	
XVII	It shall be possible to store and transfer the test results to the test result repository server in the network for record keeping	
XIX.	There shall not be any limit to number of lines of code that the tool shall review.	
XX.	The single license of tool shall be able to support testing of at least 20 devices simultaneously.	

3.2 Dynamic Application Security Testing tool:

S No.	Clauses	Complied(Yes/No)
I.	The tool shall support security testing of mobile and web applications on different platforms.	
II.	The tool shall support security testing of web services	
III.	The tool shall able to compare and report two different scans to enable a delta analysis which also includes the representation of vulnerability difference between two scans.	
IV.	The tool shall have the capability of performing vulnerability checks and tests as per OWASP top 10 related vulnerabilities.	
V.	It shall be capable to do dynamic analysis to measure statement coverage to ensure maximum coverage and having less bugs for higher assurance	
VI.	It shall be capable to do dynamic analysis to measure function coverage to ensure all	

Stamp and signature of bidder

	functions in a software programme are invoked (executed)	
VII.	It shall be capable to do dynamic analysis to measure coverage to ensure that all branches/ control in a software programme are invoked.	
VIII.	It shall be capable to do dynamic analysis at system testing level (completed programme), Module level (files contains many functions) and Unit level (files contains single function)	
IX.	It shall be capable of generating dynamic flow graphs to view system level coverage, Module level coverage and Function level coverage	
X.	It shall be possible to access the tool and conduct testing lifecycle from the User interface from the desktop client.	
XI.	It shall be possible to store and transfer the test results to the test result repository server in the network for record keeping.	
XII.	The single license of tool shall be able to support testing of atleast 20 devices simultaneously.	

4. Binary Analysis tool:

S No.	Clauses	Complied (yes/No)
I.	This tool shall be capable of evaluating vulnerabilities introduced by linked libraries, APIs, web services compiler optimizations and third party components by looking at the code in its "final" compiled version.	
II.	The supplied binary analysis tool shall be capable of detecting threats introduced as a result of malicious codes and backdoors	

Stamp and signature of bidder

	by analyzing all code paths and data flows that the program will execute.	
III.	It shall also examine communication among components for any weaknesses introduced during linkage.	
IV.	The tool shall provide reports in standard format. The generated report shall help in fixing the most severe vulnerabilities first and should point out the exact location of code creating each problem. It shall also provide supplementary details about the nature of the issue and recommend a specific fix.	
V.	The tool shall be platform independent and shall have a user friendly web based GUI. It shall also support all processing architectures prevailing at the time of supply	
VI.	It shall be updated and upgraded by the supplier for supporting the new coding languages, libraries, APIs, compiler optimizations, executable file versions and third party components used in the telecom or IT software / firmware domain including CPEs, mobile phones, applications etc. within a time frame of 3 months from the date of request by the purchaser during the entire period of contract.	
VII.	The supplier shall upgrade the tool's capabilities for scanning the executables related to new operating systems, firmware, databases, protocols and applications being used by telecom equipment, smartphones, tablets, dongles, modems, all types of wireless access points etc. within 3 months from date of request by the purchaser during the entire period of contract.	
VIII.	The supplier shall upgrade the tool's capabilities for scanning the executables related to upgraded versions of existing operating systems, firmware, databases, protocols and applications etc. already supported by the tool within 3 months of	

Stamp and signature of bidder

	their release during the entire period of contract.	
IX.	It shall be updated by the supplier for detection of new threats as per the weaknesses included in the OWASP, SANS, CWE lists etc. within a 15 days' time frame from the date of release of such additions.	
X.	It shall report for the extra executable or files which are not the part of the software release offered.	
XI.	The supplier shall provide a suitable on-site mechanism to customize the format of the report generated by the tool as per the requirement of the purchaser.	
XII.	It shall be possible to access the tool and conduct testing lifecycle from the User interface from the desktop client.	
XIII.	It shall be possible to store and transfer the test results to the test result repository server in the network for record keeping.	
XIV.	The single license of tool shall be able to support testing of atleast 20 devices simultaneously.	

5. Penetration Testing Tool:

S no.	Clauses	Complied (Yes/No)
I.	Penetration testing tool shall be capable of launching attacks on targets /systems under test for exploiting the detected vulnerabilities.	
II.	It shall determine whether the detected vulnerabilities are actually exploitable.	
III.	This tool shall correlate and prioritize results to deliver an accurate, risk-ranked list of issue to ensure that the most serious issues are addressed first. It shall generate actionable data in the form of detailed reports highlighting risks of targeted	

	systems, tests conducted, vulnerabilities exploited, and attack paths followed plus links to patches for the detected vulnerabilities and other remediation data.	
IV.	It shall have the capabilities of addressing a wide range of threat vectors related to various types of networks and end user devices.	
V.	It shall also have the capability of development of new customized exploits, as well as augmentation or modifications in the existing exploits. These customizations or modifications shall be possible without any expertise in programming languages.	
VI.	The tool shall be platform independent and shall have a user friendly web based GUI.	
VII.	The supplier shall provide a suitable on-site mechanism to customize the format of the report generated by the tool as per the requirement of the purchaser.	
VIII.	The tool shall support importing of scan result from external tools including but not limited to Nexpose, NetSparker, Nessus, Burpsuite, Acunetix, AppScan etc.	
IX.	The tool shall support brute force testing on services including but not limited to DB2, MySQL, MSSQL, HTTP, HTTPS, SSH, Telnet, FTP, POP3, SNMP.	
X.	The tool shall support web crawling on IPv4 and IPv6 web sites.	
XI.	The tool shall support detection of vulnerable URLs as per latest OWASP TOP10 standards.	
XII.	The tool shall support web crawling a minimum of 4 Websites concurrently.	
XIII.	The supplier shall update its library of exploits on a continuous basis as per the CVE catalogue updation at least once in a week. All the exploits must be thoroughly	

Stamp and signature of bidder

	tested prior to its incorporation in the SECURITY TEST lab.	
XIV.	The supplier shall continually update and upgrade its manual exploit development and customization module, on its own, as per the latest techniques and best practices available in the market, but not later than 3 months from the date of request made by the purchaser.	
XV.	It shall be possible to access the tool and conduct testing lifecycle from the User interface from the desktop client.	
XVI.	It shall be possible to store and transfer the test results to the test result repository server in the network for record keeping.	
XVII.	The single license of tool shall be able to support testing of at least 20 devices simultaneously.	

Stamp and signature of bidder